

APPENDICES

E303: Communication Systems

Professor A. Manikas
Chair of Communications and Array Processing

Imperial College London

An Overview of Fundamentals: PN-codes/signals & Spread Spectrum

Table of Contents

- 1 Introduction
 - 3GPP
 - Definition of a SSS
 - Classification of SSS
 - Modelling of $b(t)$ in SSS
 - Applications of Spread Spectrum Techniques
 - Definition of a Jammer
 - Definition of a MAI
 - Processing Gain (PG)
 - Equivalent EUE
- 2 Principles of PN-sequences
 - Comments on PN-sequences Main Properties
 - An Important "Trade-off"
- 3 m-sequences
 - Shift Registers and Primitive Polynomials
 - Implementation of an 'm-sequence'
 - Auto-Correlation Properties
 - Some Important Properties of m-sequences
 - Cross-Correlation Properties and Preferred m-sequences
 - A Note on m-sequences for CDMA
- 4 Gold Sequences
 - Introductory Comments
 - Auto-Correlation Properties
 - Cross-Correlation Properties
 - Balanced Gold Sequences
- 5 Appendices
 - Appendix A: Properties of a Purely Random Sequence
 - Appendix B: Auto and Cross Correlation functions of two PN-sequences
 - Appendix C: The concept of a 'Primitive Polynomial' in GF(2)
 - Appendix D: Finite Field - Basic Theory
 - Appendix E: Table of Irreducible Polynomials over GF(2)

Appendices

Appendix A: Properties of a purely random sequence

Let the sequence $\{\alpha[n]\}$ be the output of a discrete, memoryless source

INFORMATION SOURCE of ± 1s
$\begin{cases} P(\alpha[n] = 1) = 0.5 \\ P(\alpha[n] = -1) = 0.5 \end{cases}$

 $\rightarrow \{\alpha[n]\}$

with

$$\mathcal{E}\{\alpha[n]\} = 0 \quad (= 1 \times 0.5 + (-1) \times 0.5 = 0) \quad (29)$$

$$Var\{\alpha[n]\} = 1 \quad (= 1^2 \times 0.5 + (-1)^2 \times 0.5 = 1) \quad (30)$$

The auto-correlation of the sequence $\{\alpha[n]\}$ over M symbols is defined as follows

$$R_{\alpha\alpha}^M[k] \equiv \sum_{n=1}^M \alpha[n]\alpha[n+k] = \begin{cases} \sum_{n=1}^M \alpha[n]^2 = \sum_{n=1}^M 1 = M & k = 0 \\ \text{random} & k \neq 0 \end{cases} \quad (31)$$

Therefore the mean and the variance of the autocorrelation function $R_{\alpha\alpha}^M[k]$ are as follows

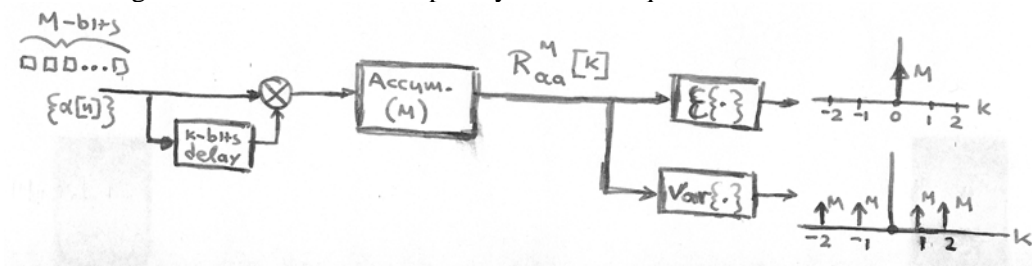
$$\mathcal{E}\{R_{\alpha\alpha}^M[k]\} = \sum_{n=1}^M \mathcal{E}\{\alpha[n]\alpha[n+k]\} = \begin{cases} \sum_{n=1}^M \mathcal{E}\{\alpha[n]^2\} = \sum_{n=1}^M 1 = M & \text{if } k = 0 \\ \sum_{n=1}^M \mathcal{E}\{\alpha[n]\}\mathcal{E}\{\alpha[n+k]\} = 0 & \text{if } k \neq 0 \end{cases} \quad (32)$$

$$\begin{aligned} Var\{R_{\alpha\alpha}^M[k]\} &= \mathcal{E}\{R_{\alpha\alpha}^M[k]^2\} - \mathcal{E}\{R_{\alpha\alpha}^M[k]\}^2 = \\ &= \sum_{n=1}^M \sum_{m=1}^M \mathcal{E}\{\alpha[n]\alpha[n+k]\alpha[m]\alpha[m+k]\} - \mathcal{E}\{R_{\alpha\alpha}^M[k]\}^2 = \\ &= \begin{cases} \sum_{n=1}^M \sum_{m=1}^M \mathcal{E}\{\alpha^2[n]\} \cdot \mathcal{E}\{\alpha^2[m]\} - \mathcal{E}\{R_{\alpha\alpha}^M[0]\}^2 = M^2 - M^2 = 0 & \text{if } k = 0 \\ \sum_{n=1}^M \mathcal{E}\{\alpha^2[n]\} \cdot \mathcal{E}\{\alpha^2[n+k]\} - \mathcal{E}\{R_{\alpha\alpha}^M[k]\}^2 = M - 0 = M & \text{if } k \neq 0 \end{cases} \end{aligned} \quad (33)$$

One may also define the cross-correlation of two sequences $\{\alpha_1[n]\}$ and $\{\alpha_2[n]\}$

$$R_{\alpha_1\alpha_2}^M[k] = \sum_{n=1}^M \alpha_1[n]\alpha_2[n+k] \quad (34)$$

Since $\{\alpha_1[n]\}$ and $\{\alpha_2[n]\}$ are independent the results are essentially the same as for the auto-correlation of $\{\alpha_1[n]\}$ with non-zero lag k . This shows that completely random sequences have nice auto- and cross-correlation properties.



Note that pure random sequences could be used as code sequences, but since the receiver needs a replica of the desired code sequence in order to despread the signal, PN sequences are used instead in practice.

Appendix B: Auto and Cross Correlation functions of two PN-sequences $\{\alpha_i[n]\}$ and $\{\alpha_j[n]\}$

- Consider the ∞ -sequences of ± 1 s of period N :

$$\{\alpha_i[n]\} = \dots, \alpha_i[N-1], \alpha_i[N], \alpha_i[1], \alpha_i[2], \dots, \alpha_i[N-1], \alpha_i[N], \alpha_i[1], \dots$$

$$\{\alpha_j[n]\} = \dots, \alpha_j[N-1], \alpha_j[N], \alpha_j[1], \alpha_j[2], \dots, \alpha_j[N-1], \alpha_j[N], \alpha_j[1], \dots$$

- Then, there are three different cross-correlation functions

$$\diamond \text{aperiodic cross-correlation: } C_{\alpha_i \alpha_j}[k] \equiv \begin{cases} \sum_{n=1}^{N-k} \alpha_i[n] \alpha_j[n+k] & 0 \leq k \leq N-1 \\ \sum_{n=1}^{N+k} \alpha_i[n-k] \alpha_j[n] & 1-N \leq k \leq 0 \\ 0 & \|k\| \geq N \end{cases} \quad (35)$$

$$\diamond \text{periodic cross-correlation: } R_{\alpha_i \alpha_j}[k] \equiv \sum_{n=1}^N \alpha_i[n] \alpha_j[n+k] \quad (36)$$

$$\diamond \text{odd cross-correlation function: } \tilde{R}_{\alpha_i \alpha_j}[k] = C_{\alpha_i \alpha_j}[k] - C_{\alpha_i \alpha_j}[k-N] \quad (37)$$

- Note that:

\diamond it is easy to see that

$$R_{\alpha_i \alpha_j}[k] = C_{\alpha_i \alpha_j}[k] + C_{\alpha_i \alpha_j}[k-N] \quad (38)$$

\diamond the periodic (or even) cross-correlation function has the property

$$R_{\alpha_i \alpha_j}[k] = R_{\alpha_i \alpha_j}[N-k] \quad (39)$$

\diamond the name of "odd cross-correlation" function follows from the property

$$\tilde{R}_{\alpha_i \alpha_j}[k] = -\tilde{R}_{\alpha_i \alpha_j}[N-k] \quad (40)$$

- For a single code sequence, the corresponding autocorrelation functions have similar properties.

- For best CDMA system performance, all $C_{\alpha_i\alpha_j}[k]$, $R_{\alpha_i\alpha_j}[k]$, $\tilde{R}_{\alpha_i\alpha_j}[k]$ should be as small as possible, since they are proportional to the interference from other users.

The out-of-phase (i.e. for lag not equal to zero) autocorrelation functions should also be made as small as possible, since these affect the multipath suppression capabilities and the acquisition and tracking performance of the receivers.

We thus define the peak cross-correlation parameters

$$\begin{cases} R_{\text{cross}} = \max \left\{ \|R_{\alpha_i\alpha_j}[k]\|, \forall (i, j, k; i < j) \right\} \\ \tilde{R}_{\text{cross}} = \max \left\{ \|\tilde{R}_{\alpha_i\alpha_j}[k]\|, \forall (i, j, k; i < j) \right\}, \\ C_{\text{cross}} = \max \left\{ \|C_{\alpha_i\alpha_j}[k]\|, \forall (i, j, k; i < j) \right\} \end{cases} \quad (41)$$

- Similarly we define the peak autocorrelation parameters

$$\begin{cases} R_{\text{auto}} = \max \left\{ \|R_{\alpha_i\alpha_i}^N[k]\|, \forall i; \forall k \neq 0(\text{mod } N) \right\}, \\ \tilde{R}_{\text{auto}} = \max \left\{ \|\tilde{R}_{\alpha_i\alpha_i}^N[k]\|, \forall i; \forall k \neq 0(\text{mod } N) \right\}, \\ C_{\text{auto}} = \max \left\{ \|C_{\alpha_i\alpha_i}^N[k]\|, \forall i; \forall k \neq 0(\text{mod } N) \right\} \end{cases} \quad (42)$$

- Finally we define

$$\begin{cases} R_{\text{peak}} = \max \{ R_{\text{auto}}, R_{\text{cross}} \} \\ \tilde{R}_{\text{peak}} = \max \{ \tilde{R}_{\text{auto}}, \tilde{R}_{\text{cross}} \} \\ C_{\text{peak}} = \max \{ C_{\text{auto}}, C_{\text{cross}} \} \end{cases} \quad (43)$$

- With the above definitions we can see that the smaller the peak correlation parameters R_{peak} , \tilde{R}_{peak} and C_{peak} , the better the performance of a system. These parameters, however, cannot be made as small as we wish. For example, for a set of K sequences of period N , according to the Welch lower bound,

$$R_{\text{peak}} \geq N \sqrt{\frac{K-1}{NK-1}} \quad C_{\text{peak}} \geq N \sqrt{\frac{K-1}{2NK-K-1}} \quad (44)$$

Therefore for large values of K and N the lower bounds on R_{peak} and C_{peak} are approximately

$$R_{\text{peak}} \geq \sqrt{N} \quad C_{\text{peak}} \geq \sqrt{\frac{N}{2}} \quad (45)$$

Moreover, it can show that

$$R_{\text{auto}}^2 + R_{\text{cross}}^2 > N \quad C_{\text{auto}}^2 + C_{\text{cross}}^2 > \frac{N}{2} \quad (46)$$

The above shows that not only is there a lower bound on the maximum correlation parameters, but also a trade-off between the peak autocorrelation and cross-correlation parameters. Thus the autocorrelation and cross-correlation functions cannot be both made small simultaneously. The design of the code sequences should be therefore very careful so that all the of above quantities of interest remain as small as possible.

Appendix C: The concept of a 'Primitive Polynomial' in GF(2) (see Appendix 4E for 'finite field' basic theory).

- Consider a polynomial $f(D)$ over the binary field GF(2): $f(D) = \underset{\substack{\uparrow \\ \neq 0}}{f_n} D^n + f_{n-1} D^{n-1} + \dots + f_1 D + f_0$

The largest power of D with non-zero coef. is called **degree** of $f(D)$ over GF(2)

- if $\underset{\substack{\uparrow \\ m}}{f(D)}, \underset{\substack{\uparrow \\ n}}{g(D)} \in \text{GF}(2)$ then $\begin{cases} f(D) + g(D) \in \text{GF}(2) \\ f(D) \cdot g(D) \in \text{GF}(2) \end{cases}$

- divisible polynomial:**

A polynomial $g(D) \in \text{GF}(2)$ is said to divide $f(D) \in \text{GF}(2)$ if $\exists h(D): f(D) = h(D) \cdot g(D)$.

Then the polynomial $f(D)$ is called divisible

- irreducible polynomial:**

A polynomial $f(D) \in \text{GF}(2)$ of degree m is called irreducible if $f(D)$ is not divisible by any polynomial over GF(2) of degree less than m but greater than zero.

(or equivalently if it cannot factored into polynomials of smaller degree whose coefs are also 0 and 1 — i.e. the polynomials belong to GF(2))

- two important properties of irreducible polynomials: if $f(D) = \text{irreducible} \Rightarrow \begin{cases} f(0) \neq 0 \\ f(D) \text{ has odd number of terms} \end{cases}$

- primitive polynomial:**

$$\text{if } \begin{cases} f(D) = \text{irreducible (of degree } m) \text{ polynomial, and} \\ f(D) \nmid (D^k - 1) \text{ i.e. } f(D) \text{ does not divide } D^k - 1 \text{ for any } k < 2^m - 1 \end{cases}$$

then $f(D) \equiv \text{primitive polynomial}$

e.g. $D^3 + D^2 + 1$; $D^4 + D + 1$

- only a small number of polynomials are *primitive*, **but** $\forall m \exists$ at least one *primitive* polynomial.

- examples: $f(D) = D^3 + D^2 + 1 = \text{primitive}$
 $f(D) = D^4 + D^2 + 1 = \text{irreducible but not primitive}$

Appendix 3.D: FINITE FIELD -BASIC THEORY

- Consider a set $S = \{s_1, s_2, \dots, s_M\}$ having M elements.

A finite field is constructed by defining two binary operations on the set called addition & multiplication such that certain conditions are satisfied. Addition and multiplication of two elements s_i and s_j are denoted $s_i + s_j$ and $s_i \cdot s_j$ respectively.

- The conditions that must be satisfied for S and the two operations to be a finite field are:

- The addition or multiplication of any two elements of S must yield an element of S .

That is, the set is closed under both addition and multiplication.

- Both addition and multiplication must be commutative $\rightarrow s_i + s_j = s_j + s_i$

- The set S must contain an **additive identity** element which will always be denoted by 0.

$$s_i + 0 = s_i$$

- The set S must contain an **additive inverse** element $-s_i$ for every element s_i

$$s_i + (-s_i) = 0$$

- The set S must contain a **multiplicative identity** element which will always be denoted by 1.

$$s_i \cdot 1 = s_i$$

- The set S must contain a **multiplicative inverse** element s_i^{-1} for every element s_i (excluding the additive identity 0)

$$s_i \cdot s_i^{-1} = 1$$

- Multiplication must be **distributive** over addition. $\rightarrow s_i + (s_j \cdot s_k) = (s_i + s_j) \cdot s_k$

- Both addition and multiplication must be **Associative**. $\rightarrow (s_i + s_j) \cdot s_k = s_i \cdot s_k + s_j \cdot s_k$

•EXAMPLE

It is easy to verify that $S = \{0, 1, 2\}$ with addition and multiplication defined as follows

modulo-3 +	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

modulo-3 ×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

is a field of 3 elements

e.g.

additive inverse $-0 = 0$

$$-1 = 2$$

$$-2 = 1$$

multiplicative inverse $1^{-1} = 1$

$$2^{-1} = 2$$

•EXAMPLE

It is easy also to verify that $S = \{0, 1\}$, with addition and multiplication defined as follows:

modulo-2 +	0	1
0	0	1
1	1	0

modulo-2 ×	0	1
0	0	0
1	0	1

is a field of 2 elements

e.g.

additive inverse $-0 = 0$

$$-1 = 1$$

multiplicative inverse $1^{-1} = 1$

- Note that $S = \{0, 1\}$ field above is the binary number field. Furthermore that addition can be performed electronically using EXCLUSIVE-OR gate and multiplication can be performed using an AND-gate.

• **An Important Result (presented without proof):**

The set of integers $S = \{0, 1, 2, \dots, M - 1\}$,

where $\begin{cases} M \text{ is prime, and} \\ \text{addition and multiplication are carried out modulo-}M \end{cases}$

is a field. These fields are called **prime fields**.

• **Subtraction and Division:**

The operations of subtraction and division are also easily defined for any field using the addition and multiplication tables, just as is done with the real-number field.

Subtraction is defined as the addition of the additive inverse and division is defined as multiplication by the multiplicative inverse.

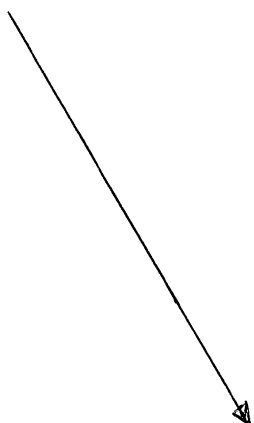
For example for the field $S = \{0, 1, 2\}$ subtraction is defined by $1 + (-2) = 1 + 1 = 2$.

Similarly, $1 \div 2 = 1 \cdot (2^{-1}) = 1 \cdot 2 = 2$.

- Note that nonprime fields do not necessarily employ modulo- M arithmetic.
- Fields can be constructed having any prime number of elements p or p^m . A field having p^m elements is called an extension field of the field having p elements.
- Finite fields are often referred to as Galois fields, using the notation $\text{GF}(M)$ for the field having M elements.
- The remainder of this discussion will be concerned exclusively with the binary number field $\text{GF}(2)$ and its extensions $\text{GF}(2^m)$. The reason for this is that the electronics used to implement the code generators is binary, and some of the shift register generators will be shown to generate the elements of $\text{GF}(2^m)$.

Appendix E: Table of Irreducible Polynomials over $\text{GF}(2)$

(from "Error-Correcting Codes" by Peterson & Weldon MIT Press, 1972)



The letters following the octal representation give the following information:

- A, B, C, D Not primitive.
- E, F, G, H Primitive.
- A, B, E, F The roots are linearly dependent.
- C, D, G, H The roots are linearly independent.
- A, C, E, G The roots of the reciprocal polynomial are linearly dependent.
- B, D, F, H The roots of the reciprocal polynomial are linearly independent.

The other numbers in the table tell the relation between the polynomials. For each degree, a primitive polynomial with a minimum number of nonzero coefficients was chosen, and this polynomial is the first in the table of polynomials of this degree. Let α denote one of its roots. Then the entry following j in the table is the minimum polynomial of α^j . The polynomials are included for each j unless for some $i < j$ either α^i and α^j are roots of the same irreducible polynomial or α^i and α^{-j} are roots of the same polynomial. The minimum polynomial of α^j is included even if it has smaller degree than is indicated for that section of the table; such polynomials are not followed by a letter in the table.

Examples. The primitive polynomial (103), or $X^6 + X + 1 = p(X)$ is the first entry in the table of sixth-degree irreducible polynomials. If α designates a root of $p(X)$, then α^3 is a root of (127) and α^5 is a root of (147). The minimum polynomial of α^9 is (015) = $X^3 + X^2 + 1$, and is of degree 3 rather than 6.

There is no entry corresponding to α^{17} . The other roots of the minimum polynomial of α^{17} are α^{34} , $\alpha^{68} = \alpha^5$, α^{10} , α^{20} , and α^{40} . Thus the minimum polynomial of α^{17} is the same as the minimum polynomial of α^5 , or (147). There is no entry corresponding to α^{13} . The other roots of the minimum polynomial $p_{13}(X)$ of α^{13} are α^{26} , α^{52} , $\alpha^{104} = \alpha^{41}$, $\alpha^{82} = \alpha^{19}$, and α^{38} . None of these is listed. The roots of the reciprocal polynomial $p_{13}^*(X)$ of $p_{13}(X)$ are $\alpha^{-13} = \alpha^{50}$, $\alpha^{-26} = \alpha^{37}$, $\alpha^{-52} = \alpha^{11}$, $\alpha^{-41} = \alpha^{22}$, $\alpha^{-19} = \alpha^{44}$ and $\alpha^{-38} = \alpha^{25}$. The minimum polynomial of α^{11} is listed as (155) or $X^6 + X^5 + X^3 + X^2 + 1$. The minimum polynomial of α^{13} is the reciprocal polynomial of this, or $p_{13}(X) = X^6 + X^4 + X^3 + X + 1$:

Appendix C Tables of Irreducible Polynomials over $GF(2)$

From Table C.2 all irreducible polynomials of degree 16 or less over $GF(2)$ can be found, and certain of their properties and relations among them are given. A primitive polynomial with a minimum number of nonzero coefficients and polynomials belonging to all possible exponents are given for each degree 17 through 34.

Polynomials are given in an octal representation. Each digit in the table represents three binary digits according to the following code:

0	000	2	010	4	100	6	110
1	001	3	011	5	101	7	111

The binary digits then are the coefficients of the polynomial, with the high-order coefficients at the left. For example, 3525 is listed as a tenth-degree polynomial. The binary equivalent of 3525 is 011101010101, and the corresponding polynomial is $X^{10} + X^9 + X^8 + X^6 + X^4 + X^2 + 1$.

The reciprocal polynomial of an irreducible polynomial is also irreducible, and the reciprocal polynomial of a primitive polynomial is primitive. Of any pair consisting of a polynomial and its reciprocal polynomial, only one is listed in the table. Each entry that is followed by a letter in the table is an irreducible polynomial of the indicated degree. For degree 2 through 16, these polynomials along with their reciprocal polynomials comprise all irreducible polynomials of that degree.

472

The exponent to which a polynomial belongs can be found as follows: If α is a primitive element of $GF(2^m)$, then the order e of α^j is

$$e = \frac{(2^m - 1)}{\text{GCD}(2^m - 1, j)}$$

and e is also the exponent to which the minimum function of α^j belongs. Thus, for example, in $GF(2^{10})$, α^{55} has order 93, since

$$93 = \frac{1023}{\text{GCD}(1023, 55)} = \frac{1023}{11}$$

Thus the polynomial (3453) belongs to 93. In this regard Table C.1 is useful.

Marsh (1957) has published a table of all irreducible polynomials of degree 19 or less over $GF(2)$. In Table C.2 the polynomials are arranged in lexicographical order; this is the most convenient form for determining whether or not a given polynomial is irreducible.

For degree 19 or less, the minimum-weight polynomials given in this table were found in Marsh's tables. For degree 19 through 34, the minimum-weight polynomial was found by a trial-and-error process in which each polynomial of weight 3, then 5, was tested. The following procedure was used to test whether a polynomial $f(X)$ of degree m is primitive:

Table C.1. Factorization of $2^m - 1$ into Primes.

$2^3 - 1 = 7$	$2^{19} - 1 = 524287$
$2^4 - 1 = 3 \times 5$	$2^{20} - 1 = 3 \times 5 \times 5 \times 11 \times 31 \times 41$
$2^5 - 1 = 31$	$2^{21} - 1 = 7 \times 7 \times 127 \times 337$
$2^6 - 1 = 3 \times 3 \times 7$	$2^{22} - 1 = 3 \times 23 \times 89 \times 683$
$2^7 - 1 = 127$	$2^{23} - 1 = 47 \times 178481$
$2^8 - 1 = 3 \times 5 \times 17$	$2^{24} - 1 = 3 \times 3 \times 5 \times 7 \times 13 \times 17 \times 241$
$2^9 - 1 = 7 \times 73$	$2^{25} - 1 = 31 \times 601 \times 1801$
$2^{10} - 1 = 3 \times 11 \times 31$	$2^{26} - 1 = 3 \times 2731 \times 8191$
$2^{11} - 1 = 23 \times 89$	$2^{27} - 1 = 7 \times 73 \times 262657$
$2^{12} - 1 = 3 \times 3 \times 5 \times 7 \times 13$	$2^{28} - 1 = 3 \times 5 \times 29 \times 43 \times 113 \times 127$
$2^{13} - 1 = 8191$	$2^{29} - 1 = 233 \times 1103 \times 2089$
$2^{14} - 1 = 3 \times 43 \times 127$	$2^{30} - 1 = 3 \times 3 \times 7 \times 11 \times 31 \times 151 \times 331$
$2^{15} - 1 = 7 \times 31 \times 151$	$2^{31} - 1 = 2147483647$
$2^{16} - 1 = 3 \times 5 \times 17 \times 257$	$2^{32} - 1 = 3 \times 5 \times 17 \times 257 \times 65537$
$2^{17} - 1 = 131071$	$2^{33} - 1 = 7 \times 23 \times 89 \times 599479$
$2^{18} - 1 = 3 \times 3 \times 3 \times 7 \times 19 \times 73$	$2^{34} - 1 = 3 \times 43691 \times 131071$

1. The residues of 1, X , X^2 , X^4 , ..., $X^{2^{m-1}}$ are formed modulo $f(X)$.
2. These are multiplied and reduced modulo $f(X)$ to form the residue of $X^{2^m} - 1$. If the result is not 1, the polynomial is rejected. If the result is 1, the test is continued.
3. For each factor r of $2^m - 1$, the residue of X^r is formed by multiplying together an appropriate combination of the residues formed in Step 1. If none of these is 1, the polynomial is primitive.

Each other polynomial in the table was found by solving for the dependence relations among its roots by the method illustrated at the end of Section 8.1.

Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.

DEGREE	15--CONTINUED	227	156053H
219	166775E	221 15143G	223 17221F
229	156745G	231 170623B	233 160373G
239	117633F	241 103605E	243 116361E
249	116135E	251 17101G	253 146212A
263	117511E	261 151541E	263 175613F
273	121125A	271 136577F	273 13227E
283	112153E	281 165033E	283 120177B
293	115153E	291 17101G	293 147037G
303	104272F	301 132111G	303 100377E
313	144275G	311 151513E	313 133777E
323	163767H	321 107177E	323 175001E
333	136237F	331 132103F	333 171033G
343	100261A	341 170277H	343 101237F
353	165355E	351 150246H	353 163533C
363	104447F	361 143001G	363 167101G
373	141655G	371 160114G	373 106715E
383	140733H	381 124205A	383 116077E
393	150225G	391 147414G	393 157111G
403	153327E	401 140573H	403 113625E
417	176735E	411 115307F	417 146356E
427	167051A	421 171755G	427 146833G
437	121212E	431 121212E	437 134037H
447	150167H	441 175665E	447 133255E
457	133571E	451 135215E	457 102212E
467	177707G	461 143501E	467 161667F
477	112407F	471 165616E	477 135715E
487	125613F	481 147133F	487 165113G
497	135017H	491 126753F	497 165077E
523	105555E	521 153425E	523 105761E
533	176147H	531 146212E	533 124767F
543	12245E	541 129221E	543 147575G
553	156065E	551 156725G	553 133737E
563	141151G	561 126015E	563 146177H
573	121855E	571 160212G	573 145361E
583	124647E	581 163761E	583 159243G
597	137253F	591 151531G	597 163456E
607	165437F	601 130578H	607 160173H
617	144115E	611 156635E	617 150613H
627	165851G	621 160305E	627 146025E
637	160530G	631 123561E	637 116423E
651	1466761C	651 135212F	651 123333E
661	146727H	661 137253F	661 143343A
671	131817F	671 125323F	671 123233E
681	120661E	681 154545E	681 135533F
691	175241G	691 160237H	691 171131E
701	122603F	701 170507G	701 160757G
715	112365E	711 146111E	711 122009F
725	135041E	721 160131E	721 122213F
735	142713C	731 102615E	731 122137F
745	163617G	741 175043E	741 132013F
755	102474E	751 164447H	751 136677F
767	177065E	761 170713E	761 155737E
777	134655E	771 152263E	771 177617G
787	126011E	781 170307F	781 174255E
807	176643H	801 130303F	801 125471E
817	163723G	811 116075E	811 150677G
827	156447H	821 125647H	821 120575E
841	144377H	841 100713E	841 121251E
851	106251E	851 116277F	851 106611E
861	130307A	861 147677G	861 164533G
871	160801E	871 126217F	871 146133E
881	127273F	881 120471E	881 162455E
891	157057H	891 162153F	891 151755E
909	173105E	901 102507F	901 176037H
919	130745E	911 173177H	911 143277F

Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.

DEGREE	15--CONTINUED	533	134205E
929	160461E	931 117137H	933 134323F
939	166737F	941 147571G	943 127743E
949	162645E	951 162403G	953 108335E
963	134755E	961 116645E	967 143307G
973	104163A	971 167753F	977 127423F
983	133041E	981 156767H	987 116037A
1057	000057E	1059 106427F	1061 113075E
1067	144713F	1069 126457E	1071 122257A
1077	177621G	1079 110741E	1081 136745E
1091	161235E	1093 144137G	1095 140675E
1101	101507E	1103 151271E	1105 157205G
1111	171125E	1113 147071A	1115 134721E
1125	133011E	1127 162337A	1129 105261E
1135	103663E	1137 146043H	1139 151403H
1145	105413F	1147 146851C	1149 165375E
1163	176657H	1165 166425E	1167 103617E
1173	165565G	1175 152135F	1177 111243E
1187	171467H	1189 150161E	1191 122011E
1197	167765C	1199 103415E	1201 137703E
1207	156257E	1209 175177H	1211 141317H
1221	127071E	1223 142457F	1225 122021A
1231	134567F	1233 156321G	1235 114335E
1241	110103E	1243 127161E	1245 163275E
1255	154445E	1257 103761E	1261 135237E
1265	127457F	1267 102205A	1269 112251E
1295	135151A	1297 106641E	1299 102265E
1305	111641E	1307 134403E	1309 102667A
1319	150231G	1321 175651G	1323 160377H
1329	163030G	1331 116675E	1333 100212E
1339	105415E	1341 122445E	1343 143631E
1353	154023H	1355 127225E	1357 176427H
1363	144225G	1365 115205A	1367 123307E
1373	101515E	1379 126023H	1381 166539E
1387	121143E	1389 111577E	1391 132747E
1397	127401E	1399 150317E	1401 177731G
1419	117715E	1421 162657H	1423 131745G
1429	153045E	1431 172155E	1433 155751E
1443	167471E	1445 141755E	1447 112535E
1453	170051G	1455 147707F	1457 160445A
1463	164121A	1465 111003F	1467 167331E
1477	140557A	1479 156673H	1481 145611E
1487	111033F	1489 172123G	1491 146667G
1497	105725E	1499 132155E	1501 150261G
1511	166267E	1513 153461E	1515 166011G
1573	176111G	1575 137331A	1577 165407G
1583	123431E	1585 172155E	1589 117731A
1593	152345E	1595 164441G	1605 172621G
1611	146203E	1613 120417E	1615 103535F
1621	140747F	1623 107037F	1625 135503E
1635	117131E	1637 105173E	1639 105071E
1645	134047A	1647 136215E	1649 153113H
1655	136335E	1657 162255E	1671 146301G
1677	157557E	1679 107711E	1681 147451E
1687	146453C	1689 172031H	1691 155213H
1701	146543E	1703 160235E	1705 166311A
1711	176013G	1713 147751G	1715 131543E
1721	144151G	1723 110433F	1733 171173F
1739	112223F	1741 116335E	1743 157165E
1749	176015G	1753 145423E	1755 114677F
1763	150327F	1765 126325E	1767 126105A
1773	170763G	1775 124175E	1777 176357F
1811	163123E	1813 151037D	1815 121431E
1821	104245E	1827 154763A	1829 152703D
1835	124071E	1837 164247H	1839 166113H
1845	106633F	1847 155437E	1849 174633H

Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.

DEGREE	15--CONTINUED	1869	157441C
1863	146701E	1865 146425E	1867 126747F
1873	142737H	1875 152301E	1877 131727E
1883	106657H	1885 152253H	1891 157645A
1897	141677G	1899 107739F	1903 135443F
1907	127177F	1909 100447E	1911 130415E
2189	161205G	2195 101131E	2197 175007G
2203	113061E	2205 102111E	2211 102763E
2217	133641E	2219 160175C	2221 161061E
2231	130737F	2235 161131E	2239 122213F
2249	117027E	2251 106273F	2253 107217E
2263	145727D	2265 121541A	2267 146607F
2277	171131G	2279 112633E	2281 137545E
2323	123163F	2325 100725A	2327 162151G
2333	132575E	2335 121211E	2337 117657F
2347	137601E	2349 143721G	2355 143727F
2361	157711G	2363 170337E	2373 166257D
2379	116057F	2381 156773H	2387 114371A
2393	151577E	2395 162713F	2397 177751G
2407	155175G	2409 103676G	2411 132015E
2421	151747G	2443 173153H	2445 111505E
2455	106745E	2457 165327H	2459 153270H
2469	150005G	2471 146007A	2473 146155E
2483	126277F	2485 103175E	2487 103175E
2501	101433F	2503 155757H	2505 121017F
2515	172363H	2517 120463E	2519 154561G
2605	147725G	2611 177527D	2613 121613E
2633	142611G	2635 110435E	2635 104575A
2645	112347F	2647 126155E	2649 131667F
2659	143531E	2661 141445E	2663 104141E
2669	111047F	2675 107121E	2677 106125E
2707	165201G	2709 106767H	2711 152351G
2717	113171E	2723 139583A	2725 175405G
2731	165355G	2733 141071E	2739 146177H
2745	153175E	2759 155407A	2761 145433H
2771	127437F	2773 176255E	2775 184445E
2787	170501E	2789 103257E	2791 120401E
2839	134255E	2841 103737E	2843 164001G
2853	110573E	2855 157511E	2857 116631E
2867	154537F	2869 143477H	2871 140755G
2889	160137E	2891 163647H	2893 121725E
2903	141125G	2905 107397A	2907 171725E
2917	154331G	2919 151607A	2921 154411E
2931	136457F	2957 126433F	2963 154515E
2969	146753E	2971 132741E	2973 145477H
3175	173655E	3177 107645E	3179 117443E
3213	131651A	3215 105233H	3217 167131H
3227	102357H	3237 163635E	3239 170277H
3245	142223G	3251 164155G	3253 117653H
3271	173737G	3273 100647E	3275 121101E
3285	144437H	3287 171737H	3289 101613F
3355	165725E	3365 110405E	3367 107675A
3373	133213E	3375 156212E	3381 114313E
3399	127077E	3401 136213E	3403 171115E
3411	116601E	3413 146737H	3417 100223E
3431	162077H	3435 150275E	3437 166755E
3477	107373E	3479 125337A	3481 110255E
3495	110501E	3497 104111E	3499 146375E
3509	121617F	3511 103333F	3513 103051E
4683	132614E	4685 142175E	4689 142175E
4709	155303H	4715 160215E	4717 162357E
4763	141171E	4771 161105E	4779 100021E
4789	123475E	4811 176135E	4813 105701E
4807	124621A	4815 123537E	4817 124317F
4941	160733H	4947 116101E	4949 114054E
5291	155707H	5293 134277F	5295 140513G

Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.

DEGREE 16---CONTINUED																
617	366345G	619	337521G	621	362745C	623	366171G	625	204227B							
627	222473B	629	233725A	631	346101G	633	261259B	635	354727B							
637	260737F	643	206603F	645	317631C	647	215343F	649	311203H							
651	221243F	653	324747H	655	310165C	657	223641F	659	323512H							
661	363271G	663	253723B	665	260145A	667	337071G	669	273361A							
671	224611E	673	267615E	675	373737D	677	316431G	679	237337F							
681	214143B	683	272071E	685	364225C	687	230371A	689	240675E							
691	306643B	693	366573B	695	235212A	697	325127H	699	241647H							
701	244333F	703	311733H	705	222127B	707	234777F	709	304535G							
711	202141A	713	256461E	715	374343D	717	341061C	719	375761G							
721	323175G	723	246041A	725	260725A	727	222017F	729	352077D							
731	212153B	733	310233B	735	210447B	737	324077H	739	306015G							
741	316757D	743	302115G	745	327031C	747	226255A	749	351225G							
751	344623H	753	211125A	755	347017D	757	320634H	759	375223D							
761	303361G	763	313751G	765	366557D	767	0000573	769	326137H							
775	256553B	777	223463B	779	302577H	781	234667F	783	225405A							
785	201171B	787	230257F	789	357617D	791	367333H	793	346243H							
795	274454A	797	325723H	799	311103D	801	310267D	803	330177H							
805	302635C	807	372301C	809	246613G	811	264507F	813	341043D							
815	275375B	817	301101G	819	262135A	821	350403H	823	367033H							
825	301347D	827	201607F	829	202607F	831	212757B	833	233155A							
835	201367B	837	222003B	839	231212E	841	200475E	843	221151A							
845	316261C	847	245265E	849	226447B	851	234155E	853	305235G							
855	222676F	857	335105G	859	227475E	861	362577D	863	274671E							
865	356471C	867	227255A	869	301213H	871	321453H	873	341645C							
875	350277D	877	240315E	879	220343B	881	343503H	883	346673H							
885	337063D	887	225737F	889	221101E	891	343547D	893	231265H							
895	315737H	897	300733D	899	270403B	901	271347B	903	356741G							
905	260775A	907	201434B	909	225051E	911	332655C	913	276241E							
915	244251E	917	211165C	919	201771E	921	305263D	923	371547D							
925	234545E	927	261141E	929	347465C	931	335205C	933	303463H							
935	356233D	937	256243F	939	337053H	941	240025A	943	346467H							
945	246683F	947	310671G	949	247457F	951	247275A	953	277047F							
955	332663H	957	367231G	959	230395A	961	355195C	963	352653H							
965	213625A	967	320225G	969	323547H	971	276031A	973	213253F							
975	226073F	977	201153B	979	333363B	981	352123D	983	367065C							
985	301451G	987	262233F	989	337553D	991	202525B	993	263737F							
995	214267B	997	212737B	1003	257507B	1005	365501C	1007	205535H							
1001	343055C	1003	344651G	1005	312454A	1007	306573D	1009	264001E							
1001	343655G	1003	201515A	1005	370743D	1007	313415G	1009	307713D							
1001	302445G	1003	222425E	1005	243083B	1007	214371E	1009	370321D							
1001	265211A	1003	365405G	1005	305301C	1007	344355C	1009	312615G							
1001	300155G	1003	331770D	1005	341703D	1007	307275G	1009	267205E							
1005	325731C	1007	376443H	1009	332033H	1101	266167B	1103	326461G							
1005	244547B	1107	212647B	1109	322171G	1111	206257F	1113	277641A							
1115	310517D	1117	312247H	1119	365307D	1121	310447H	1123	344513H							
1125	302167D	1127	337246G	1129	247475E	1131	275141A	1133	2166073A							
1135	317567D	1137	255355A	1139	353153D	1141	222633F	1143	254543B							
1145	211377H	1147	243135E	1149	377147D	1151	253207B	1153	373711G							
1155	272175E	1157	222541A	1159	226367F	1161	324439D	1163	366023D							
1165	315713H	1167	317505G	1169	325605E	1171	207307B	1173	291645A							
1175	373517D	1177	353733H	1179	327435E	1181	333515C	1183	213523F							
1185	200535E	1187	261263B	1189	373073F	1191	264463B	1193	347463D							
1185	364201G	1201	240411E	1203	274167B	1205	362715G	1207	253603B							
1209	262615A	1211	360114E	1213	315571G	1215	303045G	1217	362161C							
1223	301407H	1225	251705A	1227	215615A	1229	316505G	1231	373277H							
1233	214317B	1235	370541C	1237	313473H	1239	275651A	1241	361701C							
1243	214663F	1245	313407D	1247	216313F	1249	271655E	1251	265663B							
1253	376415G	1255	312355A	1257	355771C	1259	306235G	1261	214157F							
1263	266041A	1265	272627B	1267	216277F	1269	313677H	1271	206173B							
1273	361521G	1275	333733D	1277	0000433	1279	264637B	1281	326317H							
1291	276441E	1293	273253B	1295	341037D	1297	326715G	1299	216007H							
1301	370416E	1303	222237F	1305	224107B	1307	202277F	1309	256063B							
1311	240323B	1313	260655E	1315	266671A	1317	278765A	1319	377765A							
1321	264037F	1323	370611C	1325	300643D	1327	335675G	1329	350057D							

(degree 16, 17)

Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.

DEGREE 16---CONTINUED									
1331	353531G	1333	303367H	1335	331751C	1337	335127H	1339	354413H
1341	314651C	1343	372705C	1345	346047H	1347	3152647H	1349	255113B
1355	277341A	1357	252657F	1359	226075A	1361	330205G	1363	340065B
1365	3755127H	1367	334347H	1369	225575E	1371	324711C	1373	245025E
1375	371272D	1377	225551A	1379	341455G	1381	242167E	1383	243411A
1385	247027B	1387	230365E	1389	321165C	1391	254515E	1393	346767G
1395	242151A	1397	220217F	1399	361563H	1401	301553D	1403	332595G
1405	204351A	1411	236307B	1413	261551A	1415	375627D	1417	205273F
1419	227571B	1421	331353H	1423	200677F	1425	205237B	1427	317441G
1429	374705G	1431	205335A	1433	213631E	1435	263039B	1437	330343D
1439	243375E	1441	303013H	1443	256655A	1445	203207B	1447	242555E
1449	353045C	1451	353135G	1453	215007F	1455	302131C	1457	205247B
1459	331577H	1461	374711C	1463	245313H	1465	245247B	1467	327155C
1469	255527F	1475	256311A	1477	337555G	1479	247377B	1481	224725E
1483	355403H	1485	315407D	1487	262471E	1489	324523H	1491	302737D
1493	374471G	1495	207675A	1497	330343D	1499	330023H	1501	261765E
1503	374651C	1505	237271A	1507	265553F	1509	251327A	1511	203303F
1513	374727D	1515	374573D	1517	250737F	1519	266745E	1521	342177D
1523	255505E	1549	241317F	1551	277347B	1553	256535F	1555	224655E
1557	246455A	1559	277565E	1561	367743H	1563	240233B	1565	307563D
1567	277053F	1569	254651A	1571	213075E	1573	364077F	1575	307533D
1577	275247F	1579	202753F	1581	266517B	1583	232137A	1585	250155A
1587	371051E	1589	254551E	1591	302257H	1593	342001C	1595	252313B
1597	316145G	1603	272207F	1605	253317B	1607	223047C	1609	355519H
1611	210233H	1613	370145G	1615	356453C	1617	355147D	1619	225573F
1621	366057H	1623	243217B	1625	337252C	1627	354503H	1629	331776B
1631	364445G	1633	270616F	1635	216177H	1637	330673H	1639	271341E
1641	317373D	1643	334555E	1645	255751A	1647	312411C	1649	212423B
1651	354047H	1653	241767B	1655	351157D	1657	342721G	1659	214053B
1669	267221E	1701	305451E	1673	334539H	1675	323145C	1677	211767B
1679	236427B	1681	325275B	1683	372057D	1685	327373D	1687	277505E
1689	272713B	1691	317361G	1693	347361G	1695	220433B	1697	354213G
1699	246747F	1701	311337D	1703	220741E	1705	324051C	1707	264271A
1709	231361E	1711	254329F	1713	302505F	1715	245417B	1717	212137B
1719	360721G	1721	217671E	1723	310212G	1725	321573D	1727	336525C
1733	272677F	1735	263401A	1737	215545A	1739	204141E	1741	276117F
1743	322515F	1745	331656A	1747	244425E	1749	210656A	1751	300139C
1753	277145E	1755	332415E	1757	360456G	1759	376475G	1761	250155A
1763	261455E	1765	359525C	1767	364335C	1769	310215G	1771	210435E
1773	201557B	1775	201373B	1777	210733F	1779	204235A	1781	203603F
1783	201155E	1785	214461A	1789	000703D	1791	240435E	1803	261117B
1805	271563B	1807	242305E	1809	225753A	1811	240747A	1813	235425E
1815	262259B	1817	227647F	1819	257572D	1821	215171A	1823	343011G
1825	375333D	1827	313647D	1829	226117F	1831	326571G	1833	341523D
1835	361117D	1837	235515E	1839	344435C	1841	351021G	1843	330523H
1845	321570D	1847	347111G	1849	355329H	1851	367701C	1853	322643D
1859	344713B	1861	306733B	1863	307523F	1865	324355C	1867	303395B
1869	364203D	1871	202463F	1873	262645E	1875	232155A	1877	256353F
1879	364153H	1881	330557H	1883	247511E	1885	354415C	1887	313635C
1889	322111B	1891	314205H	1893	251765B	1895	226613B	1897	344145G
1899	330611C	1901	327373H	1903	225923F	1905	221739B	1907	205485E
1909	273235E	1911	371625C	1913	274571E	1915	227353B	1925	253215A
1927	331333H	1929	373703B	1931	270557F	1933	370467H	1935	350763D
1937	335717H	1939	211123F	1941	207163H	1943	322601G	1945	265101A
1947	377623D	1949	307273H	1951	200757F	1953	322601G	1955	265101A
1959	300205G	1959	216455A	1961	215411E	1963	331221G	1965	320151C
1967	277577F	1969	201435E	1971	332625C	1973	343335G	1975	300557D
1977	305647D	1979	355735G	1981	240477F	2115	311773D	2117	272425E
2119	247671E	2121	346173F	2123	213067F	2125	311773D	2127	205485E
2129	241775F	2131	306423H	2133	215125A	2135	342643D	2137	321439H
2139	251271A	2141	364673H	2147	211305E	2149	361371G	2151	246721A
2153	356561G	2155	222715A	2157	315225C	2159	361055C	2161	320533G
2163	214773H	2165	271215E	2167	266775F	2169	344671E	2171	274595E
2181	321917D	2183	244661E	2185	215233B	2187	215103H	2189	310009H
2191	3141427H	2193	351701C	2195	365051C	2197	335477H	2199	227311A
								(degree 16,17)	
DEGREE 24---CONTINUED									
357	1465937231C	119	123426525A	357	10573				
357	105732145A	1071	133125511A	595	15551				
1705	12170647B	1785	12170647B	595	10247				
221	100466511A	663	100006161A	663	10000				
1089	101312015A	1105	126751351A	3315	10431				
3315	104313243A	9945	116055674A	1547	15645				
4641	124430435A	4641	124430435A	1927	11263				
7735	127617123A	23205	13033563B	23205	13033				
69615	116767074A	241	174317125C	723	17122				
723	171224635C	2169	154423127D	1205	13300				
3615	154638733B	3615	154638733B	10845	15925				
16487	165365701C	5061	106342635A	5061	10634				
15183	100605077H	8435	133567111A	25305	16127				
25305	161276343B	75915	100140053H	3113	10313				
3113	1342727H	9399	131342727H	28197	16204				
15665	112155405A	46905	16411157B	46905	16411				
149083	124055647B	21931	110001100A	109655	10001				
DEGREE 25									
5	2040000051E	1	2000000011E	3	20000				
11	252001251E	7	2000101471E	15	20040				
17	200000553E	13	200014731E	21	20101				
31	2000523477H	601	353551603D	18631	27726				
1801	341513647D	55831	253566393D						
DEGREE 26									
5	430216473F	1	400000107F	3	40100				
11	426225667F	7	203265755E	9	41000				
17	471815677F	13	210664832F	15	45747				
27	471815677F	19	413535353E	33	43353				
2731	65653673D	8191	614326143D	24573	60077				

Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.

DEGREE 30	1 10040000007F	3 10065207405A
5 10104264207F	7 17254401747D	9 10466404155A
11 10421106467B	13 10115131333F	15 12531150265A
17 11326212703F	19 10343244531E	21 14340746005C
63 15671207425A	33 10617013661A	35 10617013661A
99 10231077101A	77 10347066511A	231 12551521353B
231 12551521353B	693 12363365205A	31 10537567431A
93 13104273407B	93 13104273407B	279 17565561725C
217 13063776443B	651 14475010377C	651 14475010377C
1953 16217747517D	341 15312176137D	1023 13005472403B
1023 13005472403B	3069 15027200513D	2387 17327131755A
7161 17273014127A	7161 17273014127A	21483 15222475661C
151 11732145665A	453 15642307235C	453 15642307235C
1389 13137001367A	1057 17576155211A	3171 14046056527C
3171 14046056527C	9513 15362114071A	1661 16275156545A
4983 11747625331A	4983 11747625331A	14949 14262504223C
11627 12305126259B	34881 11274077671A	34881 11274077671A
104643 16671210137D	4681 11346765601A	14043 15727555211C
14043 15727555211C	42129 11154174627A	32767 14271111643D
98301 17313775157D	98301 17313775157D	294903 17667776677D
51491 15116464137C	154473 10170400463B	154473 10170400463B
463419 13637044255B	360437 13726766575A	1081311 14437537423D
1081311 14437537423D	3243933 1765753727D	331 13214207735A
993 15100727503B	993 15100727503B	2979 11115104367B
2317 10737311047B	6951 12374572221A	6951 12374572221A
20853 11567732701A	3641 14707036127B	10923 16076273661C
10923 16076273661C	25487 10403615303A	76461 10221305567A
76461 10221305567A	10261 16150525151C	30783 10363607103A
30783 10363607103A	92349 12553152637A	71827 14221266525C
215481 17473760245C	215481 17473760245C	646443 17070134445A
112871 12527647623A	338613 12670030647A	338613 12670030647A
790097 12105065527A	2370291 10545323161A	2370291 10545323161A
49981 10400014607B	149943 10502035235A	149943 10502035235A
449829 12240170427B	349867 10101010111A	549791 11303560025A
1649373 15735076321C	1649373 15735076321C	3848537 11010100111A
1549411 12135356633B	4648233 11274767701A	4648233 11274767701A
13944699 16471647235C	10845877 11000100011A	
DEGREE 31	1 200000000011E	3 200000000017E
5 20000020411E	7 21042104211E	9 20010010017E
11 20005000251E	13 20004100071E	15 20202040217E
17 20000200435E	19 20060140231E	21 21042107357E
DEGREE 32	1 40020000007F	3 40001114005A
5 50521021747B	7 40460216667F	9 40220536125A
11 40035532523F	13 42003247143F	15 42644424505A
17 44165166133B	19 41760427607F	21 56032357221A
51 73274317525C	85 55255004227B	255 60537314115C
257 52213142567B	771 46633742135A	1285 53046115123B
3855 47254550703B	4369 45052437233B	13107 71265756301C
21845 65636126613D	65535 57410204175A	
DEGREE 33	1 100000020001E	3 100020024001E
5 104000420001E	7 100000260001A	9 100020224401E
11 111100021111E	13 100000031463F	15 104020466001E
17 100502430041E	19 100601431001E	21 100034327001A
25 100021260105A	161 107167672771A	89 100123140475A
623 124155341567B	2047 142560223461C	14329 150052442055C
599479 125725100311A	13788017 101534661265A	53353631 107753475213B
DEGREE 34	1 201000000007F	3 201051003005A
5 201472024107F	7 377000007527H	9 203123311035A
11 22521343257F	13 227712240037F	15 213753015051A
17 251132516577F	19 211636220473F	21 377235535321C
43691 327304565547D	131071 331706543633D	393213 226405640551A