A Table of Primitive Binary Polynomials

Miodrag Živković*†‡

Abstract

For those $n < 5000$, for which the factorization of $2^n - 1$ is known, the first primitive trinomial (if such exists) and a randomly generated primitive 5– and 7–nomial of degree n in GF(2) are given.

A primitive polynomial of degree n over GF(2) is useful for generating a pseudo–random sequence of n–tuples of zeros and ones, see [8]. If the polynomial has a small number k of terms, then the sequence is easily computed. But for cryptological applications (correlation attack, see [5]) it is often necessary to have the primitive polynomials with k larger than one can find in the existing tables. For example, Zierler and Brillhart [10, 11] have calculated all irreducible trinomials of degree $n \leq 1000$, with the period for some for which the factorization of $2^n - 1$ is known; Stahnke [7] has listed one example of a trinomial or pentanomial of degree $n \leq 168$; Zierler [12] has listed all primitive trinomials whose degree is a Mersenne exponent $\leq 11213 = M_{23}$ (here M_j denotes the jth Mersenne exponent); Rodemich and Rumsey [6] have listed all primitive trinomials of degree M_j, $12 \leq j \leq 17$; Kurita and Matsumoto [2] have listed all primitive trinomials of degree M_j, $24 \leq j \leq 28$, and one example of primitive pentanomials of degree M_j, $8 \leq j \leq 27$.

*1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11T06, 11T71.

†*Key words and phrases.* Primitive polynomials, finite field.

‡This research was supported by Science Fund of Serbia, grant number 0401A, through Matematički institut

Here we give (see Table 1) one primitive binary k–nomial (k–term polynomial) of degree n (if such exists and the factorization of $2^n - 1$ is known) for $2 \leq n \leq 5000$, $k \in \{3, 5, 7\}$. For chosen n and k, we have the polynomial $1 + x^n + \sum x^a$, where a takes the values from the entry at the intersection of the row n and the column k.

The 5– and 7–nomials listed in Table 1 were obtained using a random number generator. Randomly chosen k–nomials of degree n are checked for primitivity (see [9] for example) and rejected, until a primitive polynomial is found. The trinomials were tested in the natural order.

The primitivity check is carried out using the factorizations of $2^n - 1$ from [1], and also from [3] $(2^{512} + 1)$, [4] $(2^{484} + 1)$. These factorizations are known for all $n \leq 352$, and for some $n \leq 2460$, where $2^n - 1$ is not a Mersenne prime. Asterisk in front of n in Table 1 means that $2^n - 1$ contains "probably prime" factor [1], i.e. the factor without the complete primality proof.

k / n	3	5			7				
2	1								
3	1								
4	1								
5	2	1	2	3					
6	1	1	4	5					
7	1	2	3	4	1	2	3	4	5
8		1	2	7	2	4	5	6	7
9	4	3	5	6	2	3	6	7	8
10	3	2	3	8	1	2	5	6	7
11	2	1	8	10	1	2	5	7	9
12		1	2	10	2	6	8	9	10
13		3	5	8	1	2	5	10	12
14		1	11	12	1	3	4	5	11
15	1	3	4	12	5	6	7	8	13
16		10	12	15	2	9	12	13	14
17	3	4	12	16	2	5	6	8	13
18	7	4	11	16	1	4	7	8	10
19		3	9	10	6	12	13	16	18
20	3	2	7	13	1	10	14	16	18
21	2	3	4	9	6	8	14	18	19
22	1	3	7	12	2	4	9	14	21
23	5	4	8	15	5	11	12	13	17
24		2	5	11	3	6	7	16	23
25	3	7	12	13	7	10	13	15	23
26		13	15	23	1	6	15	17	24
27		17	22	23	6	11	17	18	19
28	3	5	8	24	5	11	21	24	27
29	2	2	6	16	3	11	15	16	22
30		9	10	27	11	12	24	28	29
31	3	8	23	25	1	8	10	14	16
32		2	7	16	1	3	12	17	30
33	13	11	16	26	1	8	17	19	32
34		8	12	17	4	7	14	20	31
35	2	9	17	27	2	21	23	31	32
36	11	7	12	33	6	17	25	26	28
37		2	14	22	3	21	30	31	33
38		5	6	27	6	9	11	20	36
39	4	16	23	35	2	13	15	36	38
40		23	27	29	6	7	18	28	36
41	3	27	31	32	11	12	20	32	40
42		30	31	34	1	8	14	24	27
43		5	22	27	8	25	30	32	35
44		18	35	39	5	16	25	40	43
45		4	28	39	14	15	23	27	33
46		18	31	40	21	23	24	40	44
47	5	11	24	32	5	17	19	32	42
48		1	9	19	5	12	27	29	43
49	9	16	18	24	8	39	41	42	45
50		17	31	34	5	6	16	21	36
51		15	24	46	12	15	22	24	25

Table 1: Primitive binary polynomials

k / n	3	5			7				
52	3	17	18	22	1	2	16	25	50
53		20	41	50	4	18	29	37	51
54		29	49	53	9	10	23	24	34
55	24	19	38	50	16	23	44	45	51
56		29	39	41	5	20	28	38	45
57	7	1	16	42	4	5	31	40	50
58	19	4	37	52	23	32	37	54	55
59		26	46	54	21	22	34	45	53
60	1	27	28	34	12	13	19	31	48
61		15	19	44	33	38	47	52	59
62		3	26	57	2	9	16	18	48
63	1	20	44	54	5	8	18	22	60
64		9	34	61	23	28	31	56	61
65	18	10	18	38	8	10	15	43	60
66		39	48	55	4	7	8	23	50
67		3	33	61	25	26	28	44	64
68	9	29	47	62	14	29	39	41	63
69		20	27	63	21	22	39	44	50
70		3	57	69	30	34	43	58	63
71	6	48	53	59	21	30	34	45	49
72		2	14	23	6	10	11	14	22
73	25	11	50	58	2	12	35	48	66
74		7	43	68	4	17	23	28	69
75		14	18	33	2	21	29	60	72
76		14	29	52	1	17	27	28	34
77		2	36	52	13	25	62	68	74
78		16	20	47	5	29	40	53	73
79	9	24	28	44	28	33	39	56	57
80		17	27	75	10	37	50	51	70
81	4	9	34	43	1	27	28	48	63
82		27	41	68	43	44	53	66	79
83		16	33	55	25	27	42	47	67
84	13	45	51	59	15	30	49	62	82
85		11	36	50	17	22	27	44	78
86		7	10	80	32	47	56	65	78
87	13	21	53	56	24	52	65	68	85
88		15	53	86	33	46	51	54	86
89	38	34	67	77	18	21	31	68	81
90		10	58	71	45	62	64	74	82
91		29	31	50	1	44	58	78	83
92		13	24	32	42	47	65	74	76
93	2	67	77	88	12	66	73	80	83
94	21	18	29	80	2	14	18	28	43
95	11	11	77	83	5	17	40	90	92
96		15	17	81	4	10	11	14	57
97	6	17	44	93	5	6	28	53	82
98	11	26	85	87	5	34	35	41	75
99		11	38	68	4	9	28	43	84
100	37	36	60	81	16	22	34	77	83
101		26	74	83	33	45	57	86	92

Table 1: (continued)

k / n	3	5			7				
102		15	19	27	38	50	52	65	88
103	9	60	80	83	22	35	43	67	69
104		6	49	89	33	43	80	81	102
105	16	70	87	96	7	15	21	40	101
106	15	19	86	96	12	17	34	78	86
107		39	54	59	23	29	40	84	89
108	31	3	24	59	36	43	46	62	68
109		25	58	102	3	69	74	95	100
110		21	55	97	7	17	30	70	72
111	10	5	67	77	19	54	71	101	102
112		2	19	68	63	71	87	109	111
113	9	25	80	96	13	38	48	92	109
114		54	72	103	2	38	62	74	79
115		8	20	30	17	21	47	58	98
116		24	27	95	4	11	12	43	105
117		64	73	74	4	53	70	74	104
118	33	50	106	117	29	37	45	59	109
119	8	36	52	82	20	43	92	111	116
120		9	46	88	70	71	77	82	87
121	18	33	42	43	8	25	105	115	116
122		35	39	54	93	98	100	109	119
123	2	23	51	113	4	14	18	21	121
124	37	15	31	43	48	60	72	74	107
125		65	90	103	9	24	39	57	108
126		10	70	117	51	64	70	78	81
127	1	13	45	54	31	38	67	68	97
128		11	35	77	36	38	45	57	95
129	5	2	5	10	41	43	100	110	114
130	3	19	70	97	20	46	84	110	123
131		17	28	85	32	85	87	89	104
132	29	22	43	70	5	9	83	91	93
133		28	44	50	14	21	69	101	120
134	57	34	40	71	12	18	25	69	74
135	11	10	93	109	13	17	80	88	134
136		109	114	134	9	18	39	67	106
137	21	42	56	98	1	24	44	51	99
138		26	47	103	19	24	105	109	117
139		23	60	85	35	77	91	112	118
140	29	63	97	112	3	6	39	42	69
141		7	67	125	57	64	68	81	115
142	21	67	96	137	80	85	90	104	118
143		110	118	142	10	13	17	112	136
144		54	65	129	51	53	56	66	71
145	52	23	133	138	19	55	111	124	139
146		78	101	115	22	38	46	105	116
147		43	89	110	50	118	122	141	142
148	27	27	57	124	55	98	121	129	145
149		27	60	132	33	34	53	71	148
150	53	17	62	136	69	83	87	89	94
151	3	25	27	117	7	11	33	53	64

Table 1: (continued)

k / n	3	5			7				
152		35	120	145	36	89	90	101	143
153	1	12	72	137	8	40	54	74	91
154		119	128	151	35	51	96	102	122
155		77	129	152	19	29	42	116	151
156		10	50	143	46	52	63	65	116
157		42	47	110	27	69	79	84	85
158		19	35	151	48	52	75	107	108
159	31	7	20	100	87	92	98	107	137
160		30	56	101	28	58	87	88	136
161	18	25	109	134	33	35	52	67	69
162		123	127	150	2	14	116	133	155
163		64	115	133	4	40	59	88	153
164		8	111	140	8	48	72	75	117
165		12	75	137	32	55	70	110	152
166		26	77	157	8	18	32	93	118
167	6	4	9	103	51	72	84	102	125
168		29	32	127	13	21	102	104	106
169	34	29	100	131	21	65	93	103	129
170	23	92	105	145	29	44	54	98	121
171		70	106	114	25	105	109	142	150
172	7	22	27	95	80	97	103	136	156
173		10	13	123	32	44	102	151	169
174	13	41	56	78	12	30	46	67	90
175	6	37	146	173	57	85	90	135	143
176		57	119	129	35	103	105	128	137
177	8	122	151	170	14	24	50	72	170
178	87	34	159	160	84	87	88	117	165
179		39	129	152	26	53	123	154	157
180		14	98	149	68	73	148	155	178
181		63	133	164	9	22	38	47	58
182		59	111	155	26	48	115	120	175
183	56	11	73	148	19	24	96	113	181
184		11	148	174	1	81	109	152	182
185	24	9	33	120	14	39	121	130	134
186		62	63	146	47	52	65	124	128
187		17	65	88	56	100	105	160	178
188		81	87	170	67	69	113	141	142
189		86	120	171	36	45	65	147	180
190		109	145	187	32	58	125	159	163
191	9	3	78	188	30	66	99	119	166
192		17	103	142	59	94	113	143	181
193	15	19	39	61	22	65	113	159	173
194	87	51	56	182	20	21	47	64	161
195		28	41	68	84	105	106	108	154
196		69	152	191	28	65	72	133	148
197		11	44	114	17	26	77	79	124
198	65	97	144	154	82	103	107	108	143
199	34	48	84	106	27	38	44	104	184
200		69	134	135	13	17	57	106	132
201	14	133	164	200	64	119	125	147	156

Table 1: (continued)

k / n	3	5			7				
202	55	22	63	83	90	105	117	189	195
203		121	123	167	59	85	124	133	142
204		59	95	108	97	121	140	143	162
205		147	169	197	12	103	124	174	190
206		125	129	155	3	4	88	104	199
207	43	114	126	206	28	65	129	136	167
208		63	77	97	58	64	124	159	201
209	6	78	143	204	50	63	66	98	155
210		38	47	155	13	51	62	110	190
211		52	153	155	51	63	89	114	136
212	105	29	36	176	83	92	127	158	181
213		55	84	112	15	26	64	134	135
214		88	100	133	103	176	189	191	207
215	23	41	96	124	46	74	106	125	141
216		98	103	109	31	96	133	190	207
217	45	31	51	144	12	25	81	87	144
218	11	11	95	128	27	163	165	180	212
219		55	58	143	3	37	134	190	201
220		23	121	168	39	100	134	160	190
221		142	156	211	32	69	114	154	202
222		45	46	106	44	140	157	171	180
223	33	30	64	72	44	57	85	124	169
224		2	39	116	9	132	135	203	217
225	32	57	103	205	72	93	147	178	180
226		107	128	162	65	81	96	108	137
227		11	43	142	65	100	104	189	224
228		20	100	125	44	74	127	181	220
229		4	66	189	17	55	62	112	157
230		195	212	222	24	49	96	170	201
231	26	99	137	224	13	21	118	138	174
232		35	71	169	80	150	155	180	222
233	74	41	149	189	58	65	148	185	230
234	31	37	80	113	19	113	124	146	155
235		22	37	124	20	122	160	189	234
236	5	110	117	224	73	78	86	127	141
237		54	64	211	26	31	89	144	186
238		7	44	155	72	84	93	140	178
239	36	10	56	66	12	61	207	216	226
240		226	235	238	25	31	138	150	160
241	70	28	32	170	26	100	214	217	219
242		83	91	216	29	46	66	143	170
243		97	181	191	51	94	199	203	236
244		157	190	220	18	75	119	127	210
245		193	206	243	17	107	126	137	197
246		25	147	231	55	109	184	214	226
247	82	40	96	214	12	107	151	193	220
248		53	189	199	102	107	152	178	221
249	86	40	116	146	9	65	82	113	163
250	103	28	107	180	127	139	170	175	216
251		61	75	178	110	124	199	235	249

Table 1: (continued)

k / n	3	5			7				
252	67	58	67	167	11	48	145	169	236
253		19	50	222	5	27	82	100	158
254		16	131	189	14	41	133	164	186
255	52	4	107	184	50	82	116	153	166
256		121	178	241	12	48	115	133	213
257	12	61	181	195	59	110	151	199	227
258	83	115	119	170	28	46	58	146	167
259		17	40	221	66	134	190	191	223
260		63	211	218	69	86	91	163	179
261		6	37	150	23	61	191	203	223
262		22	117	247	81	123	171	172	182
263	93	30	34	181	110	122	137	145	154
264		76	175	217	59	159	168	206	241
265	42	43	148	243	18	36	89	129	239
266	47	44	133	198	21	24	36	136	146
267		100	150	165	75	80	90	154	250
268	25	23	109	207	17	24	39	69	187
269		116	133	166	49	114	149	164	259
270	53	10	196	205	41	142	198	215	235
271	58	9	161	187	97	109	111	136	231
272		150	197	221	88	115	137	141	150
273	23	96	187	220	9	65	105	130	193
274	67	40	201	237	16	52	149	199	267
275		1	234	250	6	42	106	148	188
276		15	37	61	18	130	145	149	195
277		108	207	216	12	56	89	130	139
278	5	71	153	242	90	163	217	236	247
279	5	90	220	265	150	160	187	228	238
280		175	234	238	19	49	163	246	274
281	93	104	129	134	51	103	105	264	280
282	35	16	80	199	40	122	138	161	270
283		2	82	255	60	130	161	186	234
284	119	114	211	247	29	71	147	230	265
285		73	127	146	129	188	222	255	269
286	69	99	141	189	3	115	152	165	171
287	71	121	155	157	36	70	108	222	259
288		74	101	159	13	127	166	175	285
289	21	176	228	250	14	72	169	197	279
290		69	149	266	11	20	81	146	195
291		218	253	287	48	54	116	228	270
292	97	156	195	255	35	87	143	147	160
293		93	106	205	74	114	205	231	268
294	61	139	159	187	84	186	191	241	244
295	48	98	122	283	65	102	150	182	210
296		10	198	235	31	76	80	195	222
297	5	43	160	292	4	14	19	134	260
298		114	196	251	74	100	167	168	255
299		80	113	149	35	69	133	254	280
300	7	89	122	220	49	107	158	163	295
301		181	209	215	33	196	210	222	277

Table 1: (continued)

k / n	3	5			7				
302	41	186	189	281	61	114	182	206	277
303		43	217	274	17	77	119	215	244
304		114	145	198	56	59	74	228	235
305	102	33	63	209	140	161	230	245	300
306		119	133	244	20	52	71	86	254
307		229	237	273	33	62	81	119	306
308		51	163	229	65	126	237	282	286
309		241	286	289	6	22	146	220	300
310		84	171	211	7	113	147	251	262
312		181	238	265	171	186	195	225	283
313	79	103	133	180	66	86	119	187	262
314	15	48	64	251	39	60	116	169	207
315		21	166	259	64	113	145	185	263
316	135	42	232	267	18	20	86	174	265
317		60	227	232	76	139	166	174	227
318		35	98	201	44	101	188	303	315
319	36	44	50	144	36	135	152	233	283
320		169	293	319	9	57	233	280	295
321	31	27	70	198	78	126	149	246	299
322	67	31	234	309	48	213	233	251	321
323		7	32	106	101	202	234	247	313
324		58	169	279	56	155	158	281	321
325		20	178	245	56	71	75	239	322
326		66	107	289	88	225	258	260	301
327	34	100	154	208	9	33	243	244	301
328		10	214	289	119	134	166	213	270
329	50	219	232	301	66	151	173	175	293
330		92	247	292	52	63	195	258	267
331		50	219	298	3	25	76	130	292
332	123	227	258	281	103	120	185	205	263
333	2	40	43	110	13	21	154	255	257
334		287	325	332	132	232	269	296	331
335		193	266	307	130	166	177	213	231
336		193	235	330	2	4	19	149	274
337	55	54	137	229	21	102	112	118	258
338		203	250	303	44	97	120	126	171
339		212	237	246	69	125	219	234	236
340		222	290	317	94	183	194	267	338
341		22	49	179	103	109	234	299	333
342	125	148	152	253	240	273	281	310	316
343	75	28	68	303	29	32	228	305	340
344		29	153	211	57	92	131	145	160
345	22	241	252	279	113	129	161	230	333
346		7	40	274	27	76	138	247	325
347		37	267	334	31	64	162	209	236
348		12	122	161	72	109	123	169	298
350	53	13	238	248	103	184	237	265	278
351	34	100	147	183	49	159	221	283	308
352		134	153	313	152	168	241	285	326
354		156	183	188	11	142	222	231	308

Table 1: (continued)

k / n	3	5			7				
355		58	59	80	34	143	185	212	248
356		71	144	303	125	144	215	230	311
357		197	302	354	14	79	181	247	262
358		115	120	283	20	77	80	235	299
359	68	66	201	249	91	99	155	226	296
360		38	171	290	35	61	76	125	197
362	63	9	37	290	41	191	288	324	353
363		183	255	262	44	188	201	219	335
364	67	148	241	349	28	181	233	247	255
365		111	220	253	24	93	138	283	313
366	29	8	183	299	32	188	270	349	357
368		121	293	355	103	124	162	187	247
369	91	41	218	344	33	59	71	204	340
370	139	12	350	359	16	52	173	174	263
371		287	310	343	30	161	293	322	338
372		126	141	248	41	211	212	227	359
373		7	106	147	33	160	201	233	318
374		105	181	266	40	49	96	194	253
375	16	122	200	304	1	29	77	185	242
376		23	24	85	19	99	254	309	365
377	41	7	159	209	53	66	108	155	312
378	43	36	63	352	25	123	149	243	323
379		10	186	303	99	132	173	249	323
380	47	37	70	80	103	151	281	282	376
381		190	259	327	10	71	161	190	351
382	81	88	193	375	6	79	110	192	194
384		23	51	381	4	18	222	274	375
385	6	215	218	352	144	175	222	238	379
386	83	79	175	299	119	128	232	288	346
387		13	106	156	115	190	203	303	365
388		92	97	278	66	138	261	293	314
389		250	326	381	6	12	33	211	284
390	89	5	176	291	150	164	171	247	269
392		207	222	365	44	61	82	144	373
393	7	68	204	254	88	201	251	309	373
394	135	18	142	219	76	129	151	174	234
395		106	154	237	29	83	109	148	177
396	25	83	147	348	105	142	237	277	345
398		90	305	331	15	134	221	264	308
399	86	337	357	375	46	196	226	345	364
400		8	293	295	13	88	118	156	233
402		87	320	336	77	150	217	243	383
403		12	75	298	28	252	301	306	346
404	189	110	114	315	16	116	160	330	337
405		124	272	307	9	15	181	246	369
406	157	25	255	397	84	130	229	292	366
408		127	174	345	129	176	206	235	243
409	87	127	157	207	80	99	148	247	401
410		166	227	372	67	70	107	165	244
411		3	202	228	31	60	190	195	245

Table 1: (continued)

k / n	3	5			7				
412	147	183	360	387	130	248	325	394	404
414		106	254	281	111	117	204	261	328
415	102	90	207	351	224	295	352	394	413
416		77	196	399	94	237	282	310	365
417	107	339	404	408	82	130	235	370	378
418		120	239	259	35	181	338	348	361
420		165	278	354	66	142	239	279	341
421		296	310	329	92	138	252	280	306
422	149	94	164	253	55	101	326	404	415
424		173	211	290	133	143	292	320	360
425	12	3	109	299	66	195	223	264	269
426		107	384	407	159	186	254	351	368
427		259	264	381	18	239	323	329	364
428	105	104	178	373	162	172	180	217	410
429		282	362	383	87	96	160	220	385
430		155	187	287	26	43	69	145	416
431	120	39	47	392	11	168	179	230	247
432		111	358	430	110	120	160	170	195
433	33	125	129	263	37	82	389	392	400
434		87	257	393	75	162	177	185	377
435		78	255	307	170	175	240	369	418
436	165	90	231	249	32	125	140	172	188
437		29	130	276	157	218	252	256	398
438	65	310	324	393	81	103	184	197	231
439	49	93	162	328	1	141	392	406	427
440		193	219	292	63	75	93	215	310
441	31	49	196	404	172	195	209	225	259
442		30	199	320	120	178	182	276	423
443		34	398	420	145	147	313	366	414
444		168	313	318	119	280	339	374	376
446	105	53	59	131	62	108	204	271	400
447	73	193	299	308	21	122	259	291	293
448		49	137	143	55	73	94	202	364
450	79	320	327	435	13	50	70	128	167
451		106	215	377	69	81	207	295	364
452		101	148	237	22	118	167	396	448
453		130	152	302	213	335	370	422	451
454		12	132	429	177	281	326	355	441
455	38	54	389	433	35	108	375	402	403
456		208	209	355	123	204	231	319	370
457	16	34	124	256	3	168	193	201	303
458	203	11	223	292	12	23	47	157	161
459		2	110	281	338	341	378	387	424
460	61	128	291	404	92	184	338	364	381
461		135	257	352	67	142	314	329	332
462	73	43	92	173	28	186	214	259	393
464		10	190	285	83	234	337	426	438
465	59	13	215	370	155	327	402	442	443
466		16	76	187	48	93	126	185	460
468		173	188	440	57	66	152	246	348

Table 1: (continued)

k / n	3	5			7				
469		95	118	288	4	5	31	64	438
470	149	38	178	217	68	180	326	433	457
471	1	122	186	470	13	124	191	331	409
472		81	275	308	30	75	113	199	459
474	191	107	242	326	159	213	299	325	364
476	15	22	189	260	90	193	321	371	466
477		14	264	428	55	102	117	149	316
478	121	72	389	403	150	155	262	295	457
480		275	398	406	23	123	135	330	336
482		281	423	453	30	172	220	384	465
483		319	445	470	101	135	280	327	412
484	105	281	421	440	22	77	98	235	420
486		203	278	333	40	43	255	434	479
487	94	54	67	131	102	350	363	404	468
488		2	57	143	111	155	188	234	279
489	83	75	417	469	117	156	174	444	487
490	219	63	109	319	305	381	388	430	476
492		171	246	374	74	132	373	416	445
493		266	333	422	39	58	192	285	446
494	137	111	133	296	170	283	339	453	475
495	76	7	178	183	84	237	465	468	469
496		83	237	463	96	118	131	394	484
497	78	99	275	339	6	39	206	256	472
498		204	248	299	38	236	305	344	449
500		357	396	431	13	16	133	149	427
502		94	329	371	34	132	180	193	240
503	3	301	425	427	66	79	266	301	501
504		45	159	451	31	79	115	261	403
505	156	43	225	308	176	246	393	411	479
506	95	111	242	279	259	280	294	301	355
507		197	254	437	8	109	283	384	503
508	109	74	408	457	67	254	275	279	365
509		143	214	358	62	71	136	207	389
510		53	165	477	83	173	260	410	455
512		125	321	419	121	149	224	267	374
513	85	228	230	491	4	97	284	408	446
514		137	144	221	53	154	170	338	429
516		243	379	469	3	70	100	369	444
518	33	95	122	311	150	306	359	385	513
519	79	136	163	356	27	358	413	446	510
520		10	165	512	117	124	224	232	287
521	32	350	437	455	66	248	293	351	473
522		9	433	474	13	152	184	289	515
524	167	329	449	462	24	127	410	418	474
525		174	216	301	149	167	478	509	520
526		209	283	285	13	31	63	151	201
528		169	283	401	126	400	413	442	518
530		143	222	374	188	263	274	345	377
531		224	402	521	270	292	319	439	454
532	1	173	248	348	6	110	200	221	431

Table 1: (continued)

k / n	3	5			7				
533		181	410	457	286	307	361	492	512
534		302	326	377	22	29	411	462	503
536		119	279	302	108	140	175	474	484
537	94	82	153	222	34	51	201	224	403
538		91	168	246	305	343	384	428	461
540	179	3	431	495	72	73	152	337	429
542		222	275	487	107	193	282	302	332
544		164	175	437	75	85	173	358	394
546		35	384	486	203	256	432	446	528
547		209	422	481	152	204	244	383	413
548		354	380	445	12	76	276	300	337
549		51	222	512	38	270	369	489	539
550	193	152	186	509	3	77	101	329	521
551	135	262	326	454	27	28	84	197	388
552		5	51	305	227	232	243	280	398
553	39	88	420	506	5	144	256	296	427
554		90	203	259	25	197	316	321	497
555		7	442	553	1	25	48	413	416
556	153	47	136	446	100	124	467	488	543
558		213	256	463	56	169	365	439	499
560		357	455	465	28	52	158	432	477
561	71	182	306	479	87	260	341	381	406
562		142	196	219	10	69	73	89	317
564	163	288	337	354	10	12	127	483	545
566	153	96	257	316	14	162	173	336	557
567	143	155	255	365	113	164	204	225	498
568		35	279	430	74	238	267	388	404
570	67	81	174	347	66	188	247	341	451
572		3	71	337	61	158	337	360	562
573		130	449	496	444	449	458	467	554
574	13	185	268	557	32	145	197	512	564
575	146	13	101	466	32	153	210	376	435
576		263	330	473	354	366	391	505	529
577	25	1	57	152	162	197	289	437	495
578		171	218	282	33	68	72	217	294
579		174	212	482	25	107	154	265	338
580		36	155	239	96	130	186	283	522
582	85	57	58	313	148	221	383	388	562
583	130	79	523	567	26	92	226	420	452
584		103	155	433	39	89	99	223	445
585	121	307	432	568	252	293	295	348	523
586		80	157	377	40	143	221	285	460
588	151	302	476	513	292	306	374	408	505
590	93	75	211	313	148	294	336	437	532
591		31	109	491	242	369	405	426	554
592		1	159	499	98	355	424	513	532
594	19	212	335	506	2	125	261	469	574
595		140	413	526	107	302	418	436	493
596		142	485	568	73	293	394	480	482
597		256	452	551	29	188	214	317	569

Table 1: (continued)

k / n	3	5			7				
598		135	261	283	73	209	316	334	530
600		8	130	521	82	160	163	443	580
602		371	409	550	36	154	466	503	530
604		315	442	523	74	190	230	316	495
605		258	374	495	56	85	105	120	306
606		288	397	418	72	227	330	427	536
607	105	344	521	525	113	195	237	253	537
608		18	195	329	17	33	194	217	605
610	127	85	156	487	149	222	275	429	603
612		131	208	293	73	79	368	460	535
614		159	538	575	25	68	111	259	285
615	211	104	500	605	47	79	104	143	199
616		97	345	402	66	82	109	198	405
618		36	83	143	8	108	132	447	515
620		14	259	477	60	61	82	410	472
621		392	587	595	289	466	507	539	600
624		119	410	573	149	158	274	383	551
626		141	491	571	238	248	259	348	430
628	223	9	538	578	254	356	374	415	501
630		422	457	593	184	308	380	432	489
632		7	23	310	54	100	233	463	537
634	315	164	566	603	21	26	226	435	489
636		234	235	274	111	136	195	282	436
638		53	350	557	1	184	350	427	529
640		123	457	540	7	73	401	575	630
642	119	95	296	622	171	235	516	517	578
644		78	309	560	100	291	454	561	567
646	249	240	291	577	105	261	274	389	552
648		157	179	200	102	122	270	442	647
650	3	175	488	508	135	170	235	422	637
652	93	6	365	454	115	166	193	426	580
654		168	435	652	175	183	260	374	606
656		161	598	648	210	273	407	545	642
657	38	388	584	623	112	201	203	493	558
658	55	56	481	555	141	341	475	555	615
660		50	125	251	7	45	118	124	462
662	297	290	494	593	35	238	276	559	569
665	33	141	407	437	118	134	431	654	662
666		128	559	646	24	185	326	658	663
668		447	526	532	28	290	348	400	541
670	153	5	107	625	60	68	252	370	449
672		112	285	595	88	114	136	329	341
674		84	537	672	71	164	184	444	517
676	241	164	193	315	99	203	236	340	352
678		9	643	667	93	139	214	335	624
680		143	281	357	289	378	473	505	559
682		216	395	476	34	201	395	416	680
684		100	583	593	54	205	264	506	611
686	197	278	470	645	216	259	293	315	681
688		18	122	311	163	380	593	617	644

Table 1: (continued)

k / n	3	5			7				
690		205	211	253	106	236	483	572	663
692	299	54	263	409	8	224	239	473	557
693		2	237	327	21	297	323	398	515
694		442	477	568	163	188	460	610	645
696		271	373	498	116	191	471	526	577
697	267	238	365	677	62	240	408	503	546
700		342	458	535	68	78	405	416	663
701		58	505	693	134	152	202	289	408
702	37	401	423	446	77	171	188	381	620
704		87	143	522	39	106	303	405	440
708	287	16	335	368	58	74	79	200	232
709		407	600	637	339	407	415	638	700
710		50	257	615	3	169	348	513	643
712		139	195	490	58	280	493	548	563
714	23	257	413	440	85	508	539	663	678
715		105	242	440	183	248	292	350	554
716	183	144	465	471	323	330	402	508	534
718		264	589	625	105	271	280	338	565
720		362	531	537	250	326	403	445	493
721	9	229	700	714	109	151	451	513	659
724		91	230	317	218	387	479	507	634
726	5	469	579	619	11	345	410	444	590
728		215	693	698	18	367	422	494	608
730	147	239	349	356	164	453	492	533	702
732		425	452	688	51	88	131	281	675
735	44	119	409	629	71	250	397	454	577
738	347	62	116	573	151	326	343	405	512
740	153	16	45	563	223	279	348	393	617
742		152	371	499	19	89	181	399	635
744		93	537	635	296	312	377	720	723
745	258	10	29	368	118	159	196	198	339
747		91	425	556	295	313	395	410	468
748		309	595	683	48	55	104	287	444
750		246	321	566	43	54	157	399	648
752		15	192	749	122	217	289	432	681
753	158	47	117	296	54	131	466	550	743
754	19	176	370	395	6	171	294	354	394
755		125	535	669	90	140	409	489	567
756	349	367	474	682	31	196	205	525	573
759	98	4	246	493	147	213	465	597	608
762	83	386	503	755	14	26	309	432	587
764		48	263	670	14	172	562	693	753
768		59	504	693	61	106	494	723	758
770		179	249	550	87	179	202	505	682
771		42	597	730	34	323	649	662	702
772	7	179	639	737	111	116	165	318	634
774	185	164	254	269	8	99	117	213	534
775	367	33	697	759	2	82	410	480	529
776		166	209	447	45	246	293	457	649
778	375	206	323	601	82	307	393	514	734

Table 1: (continued)

k / n	3	5			7				
780		91	261	472	104	308	596	654	687
784		16	627	721	175	179	393	463	725
786		529	677	719	43	267	315	691	701
788		319	746	756	364	487	527	629	683
790		94	546	653	144	365	700	727	739
792		14	292	751	317	382	438	519	610
795		41	404	788	88	233	278	359	724
796		60	271	423	75	209	434	618	667
798		427	547	550	11	213	302	405	497
800		46	308	777	132	579	651	686	697
804	295	188	730	799	194	195	413	470	624
806	141	50	595	621	51	182	357	622	696
807	7	107	278	769	28	206	267	510	763
810	299	395	578	702	250	294	477	595	629
812	167	142	767	807	16	85	146	480	526
816		142	605	625	76	633	702	722	745
820		174	381	729	106	120	593	676	698
822		303	585	724	21	132	175	623	757
824		369	463	821	87	391	426	644	817
828	205	405	467	611	20	34	178	623	689
830		753	761	814	328	338	389	625	719
831	49	322	499	769	333	497	509	517	579
832		311	482	769	80	367	490	541	621
834		261	770	771	19	250	258	391	688
836		150	249	351	78	180	271	659	732
837		36	240	286	149	210	410	530	701
840		66	293	671	23	150	301	328	756
842	47	203	247	598	216	266	403	690	808
843		49	119	578	185	498	543	827	833
844		95	236	570	6	9	605	639	835
848		104	313	747	151	217	281	388	826
850	111	7	432	759	199	252	281	447	599
852		496	521	565	3	300	533	648	764
858		435	672	698	121	390	578	644	751
860		342	373	410	394	556	560	572	627
862	349	495	602	731	195	355	370	639	700
864		10	551	593	86	99	146	439	456
865	1	68	179	751	62	280	316	595	683
866	75	246	763	856	55	398	459	646	809
867		146	233	777	230	354	548	682	825
868	145	16	113	539	89	147	330	772	822
870		178	363	649	93	141	514	788	808
873		133	555	783	30	174	657	716	779
876		578	820	869	149	300	642	672	678
881	78	306	794	796	26	264	742	770	784
882		231	322	450	2	483	651	843	864
884	173	446	524	581	77	279	516	713	825
888		10	516	619	415	537	568	767	770
889	169	204	232	684	99	377	566	745	871
892	31	199	710	836	198	386	610	641	745

Table 1: (continued)

k / n	3	5			7				
894	173	17	94	623	183	241	276	386	685
896		417	726	767	109	145	338	705	884
897	113	11	425	798	50	383	546	684	792
900	1	111	771	856	156	268	348	439	739
902		27	647	874	187	255	443	542	725
903	160	489	737	809	339	393	430	659	806
904		351	431	637	62	171	242	251	754
906	187	60	421	705	32	152	626	759	887
908	143	287	384	667	22	198	575	606	867
909		110	563	654	57	439	459	554	575
910		69	489	859	96	295	304	676	799
912		277	721	731	199	330	729	779	809
916		129	508	853	17	409	525	891	900
918	77	25	481	881	280	357	378	561	790
924		63	158	753	118	154	416	463	896
930		49	52	869	275	467	664	678	823
931		325	480	921	298	647	688	830	843
932	275	119	302	864	7	162	713	802	884
936		391	639	910	16	64	134	299	627
940		83	481	654	176	255	403	453	807
942		152	842	873	255	467	609	648	876
948		269	487	569	114	174	408	625	799
952		10	275	776	283	364	510	763	765
954		26	363	888	280	303	554	586	864
956	305	342	501	582	199	337	456	639	749
960		11	221	534	103	130	136	340	802
964	103	60	697	901	268	342	413	756	800
968	0	377	610	762	160	161	330	430	879
972	115	90	252	443	345	556	641	760	957
978		679	746	808	135	381	638	671	896
979		569	713	736	129	230	346	605	832
980		171	353	732	286	579	694	712	907
984		75	686	789	260	326	425	655	950
988	121	258	351	372	536	555	616	781	850
990		283	315	610	32	170	269	298	767
996		343	478	581	36	47	336	444	639
1000		157	302	395	189	270	652	912	957
1004		678	741	923	106	384	707	930	957
1008		209	530	807	134	292	501	581	730
1010		23	272	626	181	194	537	635	725
1011		446	761	934	312	569	817	895	998
1012		37	256	996	216	260	573	938	1009
1014	385	93	484	555	308	320	550	628	877
1015	186	172	561	817	29	217	314	655	766
1020	461	146	605	900	237	304	405	485	503
1024		73	135	333	24	421	476	545	923
1026	35	401	916	929	148	331	501	705	713
1028	203	136	784	1001	130	586	735	899	924
1032		451	721	832	27	159	465	496	775
1036	411	705	769	856	1	255	707	762	831

Table 1: (continued)

k / n	3	5			7				
1044	41	184	735	738	289	477	540	799	882
1049	141	349	530	670	83	631	739	898	972
1050		579	685	735	259	626	722	1015	1035
1052	291	47	333	431	125	142	590	623	885
1056		793	854	955	286	429	433	865	994
1060		570	607	803	179	208	291	351	692
1063	168	153	314	862	23	84	248	1035	1051
1064		43	226	311	50	178	383	441	695
1066		865	954	981	43	470	673	762	1042
1068		93	932	992	30	163	357	476	623
1075		247	650	813	373	396	439	575	1049
1076		104	286	423	108	179	336	714	741
1077		56	82	935	306	577	812	991	1065
1080		43	557	1030	161	879	912	965	970
1084	189	12	940	1063	147	714	732	754	808
1085		123	522	573	77	174	321	789	938
1088		62	190	1029	34	104	178	379	982
1092	23	150	518	843	317	448	463	744	809
1098	83	115	331	371	150	468	598	723	991
1100		95	826	930	153	448	626	905	1048
1102	117	186	760	901	50	77	387	865	1037
1104		123	127	1018	166	330	436	633	929
1106	195	368	431	605	75	159	236	366	1002
1108	327	600	633	1068	635	676	738	788	1003
1110		801	813	1088	17	595	651	839	909
1116	479	522	607	996	718	728	785	997	1026
1119	283	220	605	650	144	238	378	583	591
1121	62	310	534	683	25	88	543	548	654
1122		289	758	884	53	213	249	383	505
1124		31	121	479	80	84	203	263	356
1132		226	801	1114	114	214	483	499	907
1134		262	425	662	31	74	264	441	637
1140	539	180	337	1032	234	365	520	1065	1085
1146	131	95	345	740	186	380	494	796	879
1148	23	290	516	767	42	84	387	644	826
1152		174	783	1093	121	201	422	881	1047
1155		368	605	612	131	300	315	702	864
1156	307	13	766	777	9	32	192	616	771
1158	245	819	930	1147	281	583	644	700	1075
1160		699	1013	1015	455	790	833	858	1024
1164	19	189	221	438	187	908	1083	1084	1155
1169	114	107	361	576	73	126	556	936	1076
1170		271	988	1088	61	295	752	777	875
1172		59	1050	1075	361	434	671	1037	1137
1180		237	445	764	212	364	861	1048	1091
1188	413	385	778	1152	385	660	865	894	1068
1192		331	440	545	16	194	581	1005	1104
1196	519	367	436	674	174	374	381	646	912
1200		153	319	663	48	603	782	821	952
1204		248	381	808	42	309	545	736	972

Table 1: (continued)

k / n	3	5			7				
1208		329	474	1011	11	109	627	834	918
1212	203	249	397	600	133	292	438	711	851
1220	413	820	1003	1136	15	281	587	629	1059
1224		287	290	1099	253	728	783	830	1069
1228	27	36	950	959	167	208	526	749	1185
1230		195	469	973	305	448	535	866	933
1232		193	426	725	67	322	416	857	1151
1236	151	938	989	1144	26	894	902	1159	1188
1242	395	337	449	1106	39	63	638	770	1093
1248		385	511	1031	161	310	407	700	973
1252		299	397	456	420	775	966	977	1239
1260		7	283	692	518	884	1075	1104	1251
1268		50	77	480	307	517	553	588	1148
1272		161	669	1202	35	275	591	682	847
1276	427	291	414	988	360	438	532	591	1154
1279	216	552	1080	1242	9	1013	1101	1170	1252
1284	223	125	853	1096	203	212	643	781	1246
1292		411	879	896	149	367	577	991	1171
1300	217	212	502	1031	47	332	441	679	1027
1304		255	345	578	35	108	195	531	998
1308		238	925	1184	480	536	549	1085	1268
1316		708	972	1235	381	558	948	1195	1237
1320		83	523	865	1	352	523	817	1011
1324	337	48	488	1241	97	354	702	751	1228
1332	95	939	982	1008	12	61	898	1200	1215
1340	189	84	484	1039	69	596	709	922	1176
1352		573	1199	1223	182	322	555	1063	1231
1356	275	32	571	670	420	503	916	986	1098
1364		394	609	734	123	213	253	316	659
1372	181	672	957	1144	114	178	874	1038	1371
1380		673	936	943	636	668	946	1327	1356
1384		623	642	1343	188	350	377	509	904
1386		69	881	999	125	370	657	736	1128
1400		182	515	1109	347	555	821	852	1139
1402	127	23	50	1371	64	548	868	931	1112
1404	661	149	513	1169	255	344	536	1112	1340
1420		469	725	965	567	635	872	876	1063
1428	557	79	415	439	30	55	408	683	1387
1436		201	440	711	241	347	353	834	848
1452		306	816	1345	307	858	1138	1323	1409
1456		170	362	447	138	624	827	1010	1317
1460		371	939	1303	543	943	966	1160	1200
1464		301	575	620	827	911	1138	1234	1378
1470	569	129	458	1421	123	168	505	972	1351
1476	265	44	836	1001	96	270	280	575	838
1480		367	390	845	475	842	949	965	1273
1484		417	914	1385	338	992	1144	1415	1432
1500		301	841	1291	76	169	242	347	1105
1506		75	668	1157	175	375	383	983	1011
1508	599	897	1322	1409	207	364	562	653	1326

Table 1: (continued)

References

[1] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, S. S. Wagstaf, Jr, *Factorization of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers* 2nd ed., Contemp. Math., vol. 22, Amer. Math. Soc., Providence, RI, 1988.

[2] Y. Kurita, M. Matsumoto, *Primitive t–nomials (*$t = 3, 5$*) over* GF(2) *hose degree is a Mersenne exponent* ≤ 44497, Math. Comp. **56** (1991), 817–821.

[3] A. K. Lenstra, et. al, A note in *Editor's corner*, IACR Newsletter **7** no. 2 (June 1990), 1–2.

[4] A. K. Lenstra, M. S. Manasse, *Factoring with two large primes*, in Advances in Cryptology – EUROCRYPT'90, Lecture Notes in Comput. Sci., vol. 473, Springer–Verlag, 1991, 77–82.

[5] W. Meier and O. Staffelbach, *Fast correlation attacks on certain stream ciphers*, J. Cryptology **1** (1989), 159–176.

[6] E. R. Rodemich, H. Rumsey, Jr., *Primitive trinomials of high degree*, Math. Comp. **22** (1968), 863–865.

[7] W. Stahnke, *Primitive binary polynomials*, Math. Comp. **27** (1973), 977–980.

[8] R. C. Tausworthe, *Random numbers generated by linear recurrence modulo two*, Math. Comp. **19** (1965), 201-209.

[9] E. J. Watson, *Primitive polynomials (mod* 2*)*, Math. Comp. **16** (1962), 368–369.

[10] N. Zierler, J. Brillhart, *On Primitive trinomials* (mod 2), Inform. Control **13** (1968), 541–554.

[11] N. Zierler, J. Brillhart, *On primitive trinomials* (mod 2)*, II*, Inform. Control **14** (1969), 566–569.

k / n	3	5			7				
1510		174	587	1351	207	305	856	884	909
1512		415	1100	1417	419	494	615	927	1503
1524	293	185	1143	1247	250	315	707	862	972
1540		251	583	1412	104	157	215	346	1344
1548	505	19	1052	1102	94	480	811	864	926
1556		403	434	1270	50	923	1110	1230	1365
1572		434	586	1321	815	916	969	972	1334
1584		369	931	1101	539	692	748	1106	1241
1590	169	258	481	1552	40	361	508	750	859
1596	697	363	618	1490	39	355	527	1069	1073
1600		347	725	1345	73	281	545	1133	1578
1612	771	402	524	1157	106	214	811	1215	1425
1620	227	335	1279	1331	517	738	1161	1309	1599
1644		540	772	1587	806	1318	1406	1407	1450
1656		1464	1511	1617	170	1038	1131	1408	1465
1668		227	575	1062	206	501	1136	1192	1653
1680		146	427	1349	405	922	930	1513	1579
*1688		101	406	1119	109	216	942	1159	1328
1700	311	100	891	1597	157	204	276	644	741
1716		523	571	894	145	259	479	582	1499
1732		731	1274	1716	186	196	1028	1304	1327
1734		131	365	837	226	423	514	1147	1281
1740		87	288	374	229	794	933	995	1369
1764		162	1170	1751	352	793	832	1129	1425
1784		3	25	335	10	395	838	1387	1740
1812		116	482	1059	350	507	583	1086	1507
1820	359	63	470	965	631	739	1023	1026	1694
1836		1443	1570	1827	76	1316	1348	1613	1779
1848		290	1821	1833	125	443	906	1012	1522
1860	761	23	103	950	434	726	736	1509	1520
1884		119	942	1362	13	119	761	828	1056
1896		101	875	1798	585	634	1219	1473	1524
1904		283	1108	1845	224	635	943	1108	1542
1908		1008	1112	1773	763	946	1256	1567	1769
1920		49	371	1636	47	719	757	1079	1384
1980		89	885	1152	7	214	689	1167	1521
2008		118	1333	1797	630	793	813	1695	1794
2100	1009	328	1106	1921	488	1712	1763	1964	2014
2203		370	1241	1865	89	217	781	903	1961
2212	423	530	1590	1955	660	712	1308	1701	1904
2220		1278	1479	2104	23	132	1334	1532	1691
*2232		549	1006	1957	362	419	655	908	1241
2244	415	624	1270	1611	47	522	1674	1751	2023
2268	895	337	340	1110	38	183	938	1688	2070
2281	715	605	1358	2274	851	1420	1802	1902	2151
2340		113	419	2082	227	611	740	1913	2323
2460	1169	462	555	1513	188	1233	1677	2200	2419
3217	67	1608	2097	2674	568	578	2074	2366	2880
4253		1906	2737	3392	71	1891	2023	3375	3519
4423	271	313	1506	1998	2286	2493	2877	3116	4267

Table 1: (continued)

[12] N. Zierler, *Primitive trinomials whose degree is a Mersenne exponent*, Inform. Control **15** (1969), 67–69.

Institute for applied mathematics and electronics, Beograd, Yugoslavia; mailing address is: Miodrag Živković, 11000 Beograd, Paunova 61/16, Yugoslavia.