

TABLE OF PRIMITIVE BINARY POLYNOMIALS. II

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, if the respective entry is absent from the previously published table.

After our paper with a list of primitive binary polynomials [3] had been accepted for publication, S. S. Wagstaff, Jr. made available to us reference [2] with some new factorizations of $2^n - 1$ (updates to [1] obtained up to April 5, 1993). This enabled us to make an update to our list, in which the smallest degree of missing primitive binary polynomial is now 511.

Here, like in our previous table, the degrees of nonzero coefficients (except 0 and n) of primitive k -nomials (if there are any) of degree n are given for some missing $2 \leq n \leq 5000$.

TABLE 1. Primitive binary polynomials

$n \setminus k$	3	←	5	→	←	-	7	-	→
311		26	77	206	117	127	233	245	248
349		122	289	299	52	89	179	212	240
353	69	172	234	329	107	109	186	200	229
361		18	40	227	7	82	179	217	324
367	21	136	332	335	59	174	261	270	286
383	90	270	292	380	104	132	218	225	287
391	28	202	231	316	5	35	45	213	378
397		41	184	302	21	171	182	254	373
401	152	163	224	345	136	142	186	277	320
407	71	106	236	402	88	218	275	358	359
413		151	152	232	135	165	227	244	340
419		38	120	382	10	178	219	248	266
423	25	61	181	348	45	58	145	310	385
445		129	255	420	39	198	208	363	433
449	134	263	285	359	9	104	222	243	429
463	93	151	157	253	100	191	226	293	408
467		72	103	322	60	154	326	336	345
473		73	155	304	157	197	239	275	370

Received by the editor June 11, 1993.

1991 *Mathematics Subject Classification*. 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.

TABLE 1 (continued)

$n \setminus k$	3	←	5	→	←	-	7	-	→
475		77	104	178	46	154	363	408	438
479	104	103	245	270	54	127	164	359	418
481	138	342	442	446	94	206	268	318	415
485		28	129	463	195	197	238	367	399
491		137	150	248	15	58	150	216	226
499		115	154	403	56	110	151	322	388
501		49	437	499	24	142	148	181	399
515		123	328	418	96	171	191	358	478
517		105	290	391	23	157	206	259	445
523		156	245	460	100	243	290	293	352
535		70	95	282	9	114	267	374	463
541		185	407	426	148	176	234	325	407
545	122	17	437	504	71	258	353	360	405
587		30	52	247	92	125	219	333	491
622	297	72	488	589	29	62	107	367	404
627		200	225	510	496	539	557	559	563
633	101	100	101	418	19	171	182	296	552
637		342	588	595	285	422	426	486	634
639	16	15	249	439	17	414	447	497	623
645		167	452	466	122	202	250	347	503
649	37	253	489	617	83	205	310	581	588
651		58	213	646	143	160	250	435	572
653		178	335	375	64	294	477	543	580
664		219	249	649	259	314	522	572	613
669		182	407	515	47	107	138	390	467
675		67	115	182	231	286	303	322	595
685		61	228	459	169	173	301	331	392
687	13	41	125	547	70	140	256	530	658
698	215	9	416	533	45	199	368	404	550
705	19	57	111	662	54	115	378	424	669
706		130	186	215	44	149	189	579	625
722	231	95	113	255	109	194	460	511	568
734		79	568	641	11	102	156	537	652
736		289	683	689	35	312	416	418	571
741		86	328	623	266	285	476	501	620
746	351	119	454	475	3	208	262	473	668
758		470	513	547	5	93	550	658	717
760		6	199	471	140	197	315	462	585
765		398	415	671	102	299	302	609	727
766		154	269	480	133	292	386	546	590
769	120	31	285	412	128	286	549	551	606
777	29	113	209	700	59	319	334	686	742
782	329	75	577	665	275	310	403	619	694
789		3	204	508	123	197	283	598	614
794	143	256	427	536	18	496	561	683	784
801	217	269	409	544	289	500	575	590	739
802		362	535	782	11	159	190	226	647
808		209	258	325	192	497	500	581	803
813		9	542	773	75	181	225	578	700
814	145	197	334	647	237	307	316	515	557
818	119	547	640	809	7	113	226	480	618
819		14	126	699	59	394	421	593	691
825	38	443	458	578	523	545	680	682	718
826	255	227	333	616	55	291	341	446	517
838	61	446	527	715	51	280	435	515	800
846		137	356	780	32	34	89	269	319

TABLE 1 (continued)

$n \backslash k$	3	←	5	→	←	-	7	-	→
847	136	118	333	583	21	171	229	352	445
849	253	70	400	609	260	507	533	633	798
851		395	566	700	130	158	452	502	581
854		346	429	793	135	429	478	640	753
856		249	451	780	6	192	482	629	814
869		146	304	837	294	379	447	550	746
872		257	480	507	197	382	489	615	757
874		39	545	820	37	117	494	596	727
875		445	469	576	84	220	423	658	849
878		180	488	725	200	261	493	693	762
879	11	47	514	722	35	41	135	456	842
880		427	593	741	101	373	462	635	706
885		495	631	741	5	287	337	367	754
886		29	304	423	95	227	376	708	795
890		31	479	525	194	377	449	626	797
891		131	182	523	1	553	638	811	856
898	207	109	516	888	213	257	626	798	835
901		94	119	693	100	155	188	286	675
907		94	558	583	133	213	228	552	758
914		293	534	860	14	104	207	364	715
920		65	264	475	126	379	499	624	851
921	221	320	494	884	52	366	599	711	904
922		231	508	542	73	612	635	712	835
926	365	126	657	914	1	203	273	302	365
928		157	394	547	162	325	483	732	800
934		510	565	718	89	228	374	480	850
938	207	263	535	823	61	326	337	501	767
944		305	678	689	238	270	357	417	806
946		49	213	614	56	193	249	273	606
950		525	614	711	62	77	366	460	542
955		49	490	675	208	252	431	566	611
958		85	540	596	144	363	779	873	904
962		129	302	485	115	203	334	359	936
965		121	306	437	171	175	374	507	525
966		81	196	850	112	219	479	637	893
968		51	330	909	213	263	395	678	819
970		398	417	439	211	620	670	710	952
974		130	556	857	235	314	504	737	791
975	19	246	925	949	295	335	394	418	836
976		138	195	451	112	273	372	423	543
982	277	118	200	309	110	196	226	299	853
986		456	672	851	177	214	317	757	899
987		296	506	785	206	230	284	756	849
992		469	635	750	62	484	536	896	943
994	223	459	529	978	182	278	336	919	938
998	101	97	653	736	40	50	489	654	901
1002		27	452	585	80	363	607	895	980
1006		343	737	908	93	124	139	858	952
1016		14	512	567	47	539	639	705	992
1024		558	751	1010	127	271	368	524	538
1030	93	93	117	1000	54	109	149	390	816
1034	75	7	390	698	287	288	378	843	974
1040		95	138	903	310	611	647	681	769

TABLE 1 (continued)

$n \backslash k$	3	←	5	→	←	-	7	-	→
1041	412	108	167	515	374	661	764	786	930
1046		164	297	301	354	365	592	836	919
1047	10	15	795	869	115	701	723	741	752
1053		405	454	801	99	478	585	615	672
1057	198	3	122	1007	187	559	655	787	948
1062		123	183	917	133	206	397	529	571
1074		703	1048	1066	132	316	331	738	1005
1082	407	82	199	278	3	82	391	535	863
1090	79	167	578	808	656	766	884	947	983
1094	261	312	645	1080	128	189	442	553	951
1103	65	30	178	925	661	771	800	862	864
1107		380	577	823	19	129	184	257	662
1120		294	718	865	165	285	456	568	767
1128		113	154	577	121	148	163	255	483
1154	75	510	953	1105	83	729	766	771	1029
1166	189	732	817	878	309	450	564	881	942
1168		299	713	1126	231	586	629	682	1097
1182		145	411	925	61	320	445	879	1149
1185	134	452	750	783	195	206	427	745	1115
1190	233	139	484	1119	62	202	477	611	731
1210	243	258	419	860	193	333	503	760	800
1244		652	786	997	227	548	820	1139	1146
1254		385	784	1022	358	660	708	997	1105
1290		70	235	842	196	566	643	887	1259
1296		579	583	1273	80	292	473	712	855
1302	325	537	668	879	197	535	687	926	1194
1314		21	320	611	39	154	591	988	1124
1328		726	1201	1225	97	573	677	843	1125
1338	511	207	288	305	475	601	857	1138	1255
1348	553	416	417	661	444	572	1072	1104	1293
1350		865	876	985	162	208	211	933	1285
1374		485	514	637	371	413	781	908	1097
1388		178	215	394	167	332	986	1233	1288
1392		551	635	853	46	479	728	1156	1263
1396	339	129	598	1186	322	792	812	833	1056
1410	383	106	399	555	464	533	667	1168	1228
1412	153	802	901	1394	406	484	765	1059	1326
1440		249	904	1347	150	831	1006	1011	1245
1444		328	562	1135	438	999	1005	1168	1338
1468	181	709	932	1214	226	255	472	520	951
1482		550	964	1351	240	401	802	1142	1234
1492		435	649	1064	3	135	348	924	1339
1504		282	465	817	510	755	830	980	1019
1516		22	378	1427	8	275	862	993	1421
1518		1183	1421	1466	35	121	261	745	923
1532		488	570	1333	57	389	1137	1309	1474
1536		647	882	1313	240	431	710	1149	1170
1538		375	1065	1452	120	555	840	1218	1478
1554		290	1124	1223	116	377	435	628	1161
1564	7	120	1005	1146	66	187	273	643	709
1568		468	661	1330	137	258	460	1045	1139
1578	731	396	1103	1400	1101	1104	1329	1336	1446
1580	647	54	311	579	222	398	442	1365	1393

TABLE 1 (continued)

$n \backslash k$	3	←	5	→	←	-	7	-	→
1588	159	3	152	355	367	707	743	1116	1498
1604		608	745	1498	188	226	661	980	1583
1616		14	836	1197	75	153	421	499	1166
1636	37	192	577	1370	35	514	904	1156	1433
1638	397	233	1242	1394	21	327	955	996	1297
1652		116	994	1359	160	342	1124	1302	1519
1660	37	76	1108	1159	163	519	842	1102	1207
1674	755	149	600	1473	454	526	1023	1076	1163
1692		168	229	1375	60	322	441	1074	1504
1724		1107	1334	1392	311	614	868	872	1366
1728		61	1112	1582	72	648	701	850	1409
1736		37	422	1471	1109	1303	1398	1657	1675
1744		131	624	1637	117	285	309	721	882
1756	99	351	1128	1359	383	636	648	824	864
1758		477	958	1512	23	51	615	739	1064
1770	607	775	1034	1315	630	693	1078	1203	1489
1772		49	287	399	58	133	260	364	456
1780	457	1	605	1173	623	637	656	970	1075
1782		334	719	1249	43	661	1390	1671	1770
1788		394	507	994	338	931	1175	1513	1632
1794		315	562	1003	25	86	246	1420	1605
1802	843	324	346	919	262	604	758	1105	1209
1824		627	1026	1541	531	544	580	1260	1473
1876		372	1377	1843	10	581	917	1293	1643
1880		433	1545	1775	129	927	1011	1650	1850
1892		364	740	1485	327	806	1004	1272	1670
1900	297	208	949	1776	145	781	1421	1656	1891
1932	277	445	1492	1838	611	1161	1247	1742	1800
1940	113	982	1532	1741	253	731	1109	1477	1632
1952		619	1109	1741	530	1065	1196	1461	1950
1956		457	696	942	514	963	993	1428	1530
1988		759	910	1805	262	1194	1518	1794	1909
1992		452	673	799	25	373	461	739	1333
2004		384	1531	1701	357	789	1204	1355	1984
2020		109	1130	1554	40	684	788	1379	1397
2028	301	27	337	480	978	1251	1269	1527	1802
2032		2	1492	1565	155	286	664	1532	1909
2040		225	398	785	210	1084	1116	1403	1555
2052		529	730	1742	433	1139	1214	1468	1534
2060	987	464	1567	1921	739	900	1187	1915	1950
2068		293	1063	1098	17	751	1106	1119	1304
2094		577	1505	1555	334	557	683	748	787
2106	931	1419	1577	1764	405	695	854	941	1019
2120		279	1351	1753	77	283	1143	1279	1991
2124		1243	1330	1566	106	400	1275	1542	2042
2160		937	1051	1558	1552	1634	1647	1688	1965
2164		320	1529	1773	548	644	895	1112	1850
2196	539	1230	1301	2168	277	302	303	358	662
2204		351	1394	1926	262	702	1138	1377	1899
2242	7	216	1091	1703	131	823	1578	1676	1725
2280		307	513	1320	76	116	298	341	1839
2292	157	257	367	2275	1061	1284	1351	1363	1488
2312		918	1145	1725	2	129	900	1526	2265

TABLE 1 (continued)

$n \setminus k$	3	←	5	→	←	-	7	-	→
2364	643	100	324	955	281	1244	1628	1792	2143
2370		747	992	2342	17	462	972	1024	2303
2380	93	124	724	1359	999	1146	1478	1586	1737
2384		621	977	1566	489	971	1026	1238	1610
2400		515	525	942	195	839	1158	1309	2138
2420		1371	2074	2396	893	981	1037	2328	2369
2484		115	1672	2432	586	626	1286	1426	1899
2580		391	580	1339	993	1580	1877	2051	2201
2604		175	1088	1957	30	288	391	1469	2035
2628		124	597	1789	277	784	977	1877	2063
2676		2314	2321	2396	481	805	908	2053	2177
2700		14	112	1757	465	471	622	1130	2387
2772		2561	2652	2705	584	911	1133	1228	2260
2940	563	1610	2353	2534	397	554	635	1376	2680
2964		1553	2634	2844	271	612	672	687	1675
3036	1087	1295	2045	2955	188	2116	2134	2137	2812
3108	947	496	1148	2425	82	490	1163	1186	2419
3180		303	588	3110	18	19	1378	2271	2998
3276	1471	156	1471	2422	53	1606	2008	2492	2594
3540		1623	2626	3391	36	72	752	1447	3527
3604	1419	137	338	2380	172	1431	2035	2515	2744

BIBLIOGRAPHY

1. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, 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. S. S. Wagstaff, Jr, *Update 2.6 to the second edition of factorization of $b^n \pm 1$* , 1993.
3. M. Živković, *A table of primitive binary polynomials*, Math. Comp. **62** (1994), 385–386.

INSTITUTE OF APPLIED MATHEMATICS AND ELECTRONICS, BEOGRAD, YUGOSLAVIA

MARKA ČELEBONVIĆA 61/15, 11070 NOVI BEOGRAD, YUGOSLAVIA