PETERSON'S TABLE OF IRREDUCIBLE POLYNOMIALS OVER GF(2)

This table was taken from **Error-Correcting Codes** by W. Wesley Peterson, MIT Press (1970), pages 251 - 155. This table is to be used only by students of ECE6604 for instructional purposes only.

From the following tables 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 is 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	0 0 0	2	0 1 0	4	1 0 0	6	1 1 0
1	0 0 1	3	0 1 1	5	1 0 1	7	1 1 1

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 loth-degree polynomial. The binary equivalent of 3525 is 0 1 1 1 0 1 0 1 0 1 0 1, 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.

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 a denote one of its roots. Then the entry following j in the table is the minimum polynomial of a^j. The polynomials are included for each j unless for some i < j either a^i and a^j are roots of the same irreducible polynomial or a^i and a^{-j} are roots of the same polynomial. The minimum polynomial of a^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 6^{th}-degree irreducible polynomials. If a designates a root of p(X), then a 3 is a root of (127) and a^5 is a root of (147). The minimum polynomial of a^9 is (015) = $X^3 + X^2 + 1$, and is of degree 3 rather than 6.

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

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

$$e = (2^m-1)/GCD(2^m-1, j)$$

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

$$93 = 1023/GCD(1023, 55) = 1023/11$$

Thus the polynomial (3453) belongs to 93.

Marsh has published a table of all irreducible polynomials of degree 19 or less over GF(2). In this table 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.

1. The residues of 1, X, X^2, X^4, ... , X^{2m-1} are formed modulo f(X).

2. These are multiplied and reduced modulo f(X) to form the residue of X^{2m-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 in Peterson.

Table Factorization of 2^m-1 into Primes

2^3 - 1	= 7	2^{19} - 1	= 524287
2^4 - 1	= 3x5	2^{20} - 1	= 3x5x5xl1x31x41
2^5 - 1	= 31	2^{21} - 1	= 7X7X127x337
2^6 - 1	= 3x3x7	2^{22} - 1	= 3x23x89x683
2^7 - 1	= 127	2^{23} - 1	= 47x178481
2^8 - 1	= 3x5x17	2^{24} - 1	= 3x3x5x7x13x17x241
2^9 - 1	= 7x73	2^{25} - 1	= 31x601x1801
2^{10} - 1	= 3x11x3	2^{26} - 1	= 3x2731x8191
2^{11} - 1	= 23x89	2^{27} - 1	= 7x73x262657
2^{12} - 1	= 3x3x5x7x13	2^{28} - 1	= 3x5x29x43x113x127
2^{13} - 1	= 8191	2^{29} - 1	= 233x1103x2089
2^{14} - 1	= 3x43x127	2^{30} - 1	= 3x3x7x11x31x151x331
2^{15} - 1	= 7x31x15	2^{31} - 1	= 2147483647
2^{16} - 1	= 3x5x17x257	2^{32} - 1	= 3x5x17x257x65537
2^{17} - 1	= 131071	2^{33} - 1	= 7x23x89x599479
2^{18} - 1	= 3x3x3x7xl9x73	2^{34} - 1	= 3x43691x131071

DEGREE	2	1	7H								
DEGREE	3	1	13F								
DEGREE	4	1	23F	3	37D	5	07				
DEGREE	5	1	45E	3	75G	5	67H				
DEGREE	6	1	103F	3	1278	5	147H	7	111A	9	015
11	155E	21	007								
DEGREE	7	1	211E	3	217E	5	235E	7	367H	9	277E
11	325G	13	203F	19	313H	21	345G				
DEGREE	8	1	435E	3	567B	5	763D	7	551E	9	675C
11	747H	13	453F	15	727D	17	023	19	545E	21	613D
23	543F	25	433B	27	477B	37	537F	43	703H	45	471A
51	037	85	007								
DEGREE	9	1	1021E	3	1131E	5	1461G	7	1231A	9	1423G
11	1055E	13	1167F	15	1541E	17	1333F	19	1605G	21	1027A
23	1751E	25	1743H	27	1617H	29	1553H	35	1401C	37	1157F
39	1715E	41	1563H	43	1713H	45	1175E	51	1725G	53	1225E

55	1275E	73	0013	75	1773G	77	1511C	83	1425G	85	1267E

DEGREE	10	1	2011E	3	2017B	5	2415E	7	3771G	9	2257B
11	2065A	13	2157F	15	2653B	17	3515G	19	2773F	21	3753D
23	2033F	25	2443F	27	3573D	29	2461E	31	3043D	33	0075C
35	3023H	37	3543F	39	21078	41	2745E	43	2431E	45	3061C
47	3177H	49	3525G	51	2547B	53	2617F	55	3453D	57	3121C
59	3471G	69	2701A	71	3323H	73	3507H	75	2437B	77	2413B
83	3623H	85	2707E	87	2311A	89	2327F	91	3265G	93	3777D
99	0067	101	2055E	103	3575G	105	3607C	107	3171G	109	2047F
147	2355A	149	3025G	155	2251A	165	0051	171	3315C	173	3337H
179	3211G	341	0007								

DEGREE	11	1	4005E	3	4445E	5	4215E	7	4055E	9	6015G
11	7413H	13	4143F	15	4563F	17	4053F	19	5023F	21	5623F
23	4757B	25	4577F	27	6233H	29	6673H	31	7237H	33	7335G
35	4505E	37	5337F	39	5263F	41	5361E	43	5171E	45	6637H
47	7173H	49	5711E	51	5221E	53	6307H	55	6211G	57	5747F
59	4533F	61	4341E	67	6711G	69	6777D	71	7715G	73	6343H
75	6227H	77	6263H	79	5235E	81	7431G	83	6455G	85	5247F
87	5265E	89	5343B	91	4767F	93	5607F	99	4603F	101	6561G
103	7107H	105	704IG	107	4251E	109	5675E	111	4173F	113	4707F
115	7311C	117	5463F	119	5755E	137	6675G	139	7655G	141	5531E
147	7243H	149	762IG	151	7161G	153	4731E	155	4451E	157	6557H
163	7745G	165	7317H	167	5205E	169	4565E	171	6765G	173	7535G
179	4653F	181	5411E	183	5545E	185	7565G	199	6543H	201	5613F
203	6013H	205	7647H	211	6507H	213	6037H	215	7363H	217	7201G
219	7273H	293	7723H	299	4303B	301	5007F	307	7555G	309	4261E
331	6447H	333	5141E	339	7461G	341	5253F				

DEGREE	12	1	10123F	3	12133B	5	10115A	7	121538	9	11765A
11	15647E	13	12513B	15	13077B	17	16533H	19	16047H	21	10065A
23	11015E	25	13377B	27	14405A	29	14127H	31	17673H	33	13311A
35	10377B	37	13565E	39	13321A	41	15341G	43	15053H	45	15173C
47	15621E	49	17703C	51	10355A	53	15321G	55	10201A	57	12331A
59	11417E	61	13505E	63	10761A	65	00141	67	13275E	69	16663C
71	11471E	73	16237E	75	16267D	77	15115C	79	12515E	81	17545C
83	12255E	85	11673B	87	17361A	89	11271E	91	10011A	93	14755C
95	17705A	97	1712IG	99	17323D	101	14227H	103	12117E	105	13617A
107	14135G	109	14711G	Ill	15415C	113	13131E	115	13223A	117	16475C
119	14315C	121	16521E	123	13475A	133	114338	135	10571A	137	15437G
139	12067F	141	13571A	143	12111A	145	16535C	147	17657D	149	12147F
151	14717F	153	13517B	155	14241C	157	14675G	163	10663F	165	10621A
167	16115G	169	16547C	171	10213B	173	12247E	175	16757D	177	16017C
179	17675E	181	10151E	183	14111A	185	14037A	187	14613H	189	13535A
195	00165	197	11441E	199	10321E	201	14067D	203	13157B	205	14513D
207	10603A	209	11067F	211	14433F	213	16457D	215	10653B	217	13563B
219	116578	221	17513C	227	12753F	229	13431E	231	10167B	233	11313F
235	11411A	237	13737B	239	13425E	273	00023	275	14601C	277	16021G
279	16137D	281	17025G	283	15723F	285	17141A	291	15775A	293	11477F
295	11463B	297	17073C	299	16401C	301	12315A	307	14221E	309	11763B
311	12705E	313	14357F	315	17777D	325	00163	327	17233D	329	11637B
331	16407F	333	11703A	339	16003C	341	11561E	343	12673B	345	14537D
347	1771IG	349	13701E	355	10467B	357	15347C	359	11075E	361	16363F
363	11045A	365	11265A	371	14043D	397	12727F	403	14373D	405	13003B
407	17057G	409	10437F	411	10077B	421	14271G	423	14313D	425	14155C
427	10245A	429	11073B	435	10743B	437	12623F	439	12007F	441	15353D
455	00111	585	00013	587	14545G	589	1631IG	595	13413A	597	12265A
603	14411C	613	15413H	619	17147F	661	10605E	683	10737F	685	16355C

691	15701G	693	12345A	715	00133	717	16571C	819	00037	1365	00007

DEGREE	13	1	20033F	3	23261E	5	24623F	7	23517F	9	30741G
11	21643F	13	3017IG	15	21277F	17	27777F	19	35051G	21	34723H
23	34047H	25	32535G	27	31425G	29	37505G	31	36515G	33	26077F
35	35673H	37	20635E	39	33763H	41	25745E	43	36575G	45	26653F
47	21133F	49	22441E	51	30417H	53	32517H	55	37335G	57	25327F
59	23231E	61	25511E	63	26533F	65	33343H	67	33727H	69	27271E
71	25017F	73	26041E	75	21103F	77	27263F	79	24513F	81	32311G
83	31743H	85	24037F	87	30711G	89	32641G	91	24657F	93	32437H
95	20213F	97	25633F	99	31303H	101	22525E	103	34627H	105	25775E
107	21607F	109	25363F	Ill	27217F	113	33741G	115	37611G	117	23077F
119	21263F	121	31011G	123	27051E	125	35477H	131	3415IG	133	27405E
135	34641G	137	32445G	139	36375G	141	22675E	143	36073H	145	35121G
147	3650IG	149	33057H	151	36403H	153	35567H	155	23167F	157	36217H
159	22233F	161	32333H	163	24703F	165	33163H	167	32757H	169	23761E
171	24031E	173	30025G	175	37145G	177	31327H	179	27221E	181	25577F
183	22203F	185	37437H	187	27537F	189	31035G	195	24763F	197	20245E
199	20503F	201	20761E	203	25555E	205	30357H	207	33037H	209	34401G
211	32715G	213	21447F	215	27421E	217	20363F	219	3350IG	221	20425E
223	32347H	225	20677F	227	22307F	229	33441G	231	33643H	233	24165E
235	27427F	237	24601E	239	36721G	241	34363H	243	21673F	245	32167H
247	21661E	265	33357H	267	26341E	269	31653H	271	37511G	273	23003F
275	22657F	277	25035E	279	23267F	281	34005G	283	34555G	285	24205E
291	26611E	293	3267IG	295	25245E	297	31407H	299	33471G	301	22613F
303	35645G	305	3237IG	307	34517H	309	26225E	311	35561G	313	25663F
315	24043F	317	30643H	323	20157F	325	37151G	327	24667F	329	33325G
331	32467H	333	30667H	335	22631E	337	26617F	339	20275E	341	36625G
343	20341E	345	37527H	347	31333H	349	31071G	355	23353F	357	26243F
359	21453F	361	36015G	363	36667H	365	34767H	367	34341G	369	34547H
371	35465G	373	24421E	375	23563F	377	36037H	391	31267H	393	27133F
395	30705G	397	30465G	399	35315G	401	3223IG	403	32207H	405	26101E
407	22567F	409	21755E	411	22455E	413	33705G	419	37621G	421	21405E
423	30117H	425	23021E	427	21525E	429	36465G	431	33013H	433	27531E
435	24675E	437	33133H	439	34261G	441	33405G	443	34655G	453	32173H
455	33455G	457	35165G	459	22705E	461	37123H	463	27111E	465	35455G
467	31457H	469	23055E	471	30777H	473	37653H	475	24325E	477	31251G
547	35163H	549	33433H	551	37243H	553	27515E	555	32137H	557	26743F
563	30277H	565	20627F	567	35057H	569	24315E	571	24727F	581	30331G
583	34273H	585	23207F	587	31113H	589	36023H	595	27373F	597	20737F
599	36235G	601	21575E	603	26215E	605	21211E	611	20311E	613	34003H
615	34027H	617	20065E	619	22051E	621	22127F	627	23621E	629	24465E
651	26457F	653	31201G	659	34035G	661	27227F	663	22561E	665	21615E
667	22013F	669	23365E	675	26213F	677	26775E	679	32635G	681	33631G
683	32743H	685	31767H	691	34413H	693	22037F	695	30651G	697	26565E
711	22141E	713	22471E	715	35271G	717	37445G	723	22717F	725	26505E
727	24411E	729	24575E	731	23707F	733	25173F	739	21367F	741	25161E
743	24147F	793	36307H	795	24417F	805	20237F	807	36771G	809	37327H
811	27735E	813	31223H	819	36373H	821	33121G	823	32751G	825	33523H

....