MATHEMATICS OF COMPUTATION
VOLUME 46, NUMBER 173
JANUARY 1986, PAGES 321-331

A Generalization of Swan's Theorem

By Harold M. Fredricksen, Alfred W. Hales and Melvin M. Sweet

Abstract. Let f and g denote polynomials over the two-element field. In this paper we show that the parity of the number of irreducible factors of $x^n f + g$ is a periodic function of n, with period dividing eight times the period of the polynomial $f^2(x(g/f)' - n(g/f))$. This can be considered a generalization of Swan's trinomial theorem [3].

1. Introduction. Let f and g denote polynomials in x over the two-element field F_2, i.e., members of $F_2[x]$. Let $r = r_n$ denote the number of irreducible factors of the polynomial $x^n f + g$. In this paper we show that, for fixed f and g, the *parity* of r_n is an eventually periodic function of n. For fixed parity of n this period is a divisor of 8π, where π is the period (in the usual sense) of the polynomial

$$h = f^2\big(x(g/f)' - n(g/f)\big),$$

i.e., the least π so that the polynomial h divides (a power of x times) $x^\pi - 1$. Our result can be considered a generalization of Swan's theorem [3] concerning the number of irreducible factors of a trinomial $x^n + x^k + 1$ (by taking $f = 1$ and $g = x^k + 1$).

We also investigate initial tail effects and some observed antiperiodicity properties of (the parity of) r_n. The paper concludes with tables of values of r_n for various f, g, and n.

We wish to thank Lloyd Welch for providing us with a polynomial factoring program. This program was an immense help in checking and refining our results.

2. Background. We begin by recalling various properties of the resultant and discriminant for polynomials F, G with integer coefficients [1]. If

$$F(x) = a\prod_{i=1}^{n}(x - \alpha_i) \quad \text{and} \quad G(x) = b\prod_{j=1}^{m}(x - \beta_j),$$

then the *resultant* $R(F,G)$ is an integer given by any one of the following equal expressions:

$$R(F,G) = a^m b^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j), \tag{1}$$

$$R(F,G) = a^m \prod_{i=1}^{n} G(\alpha_i), \tag{2}$$

$$R(F,G) = (-1)^{mn} b^n \prod_{j=1}^{m} F(\beta_j). \tag{3}$$

Received July 10, 1984.
1980 *Mathematics Subject Classification*. Primary 12C05.

$R(F,G)$ is also the value of the determinant of the following $(m+n)\times(m+n)$ matrix where

$$F(x)=ax^n+a_1x^{n-1}+\cdots+a_n \quad \text{and} \quad G(x)=bx^m+b_1x^{m-1}+\cdots+b_m:$$

$$\begin{array}{cccccccccc}
a & a_1 & \cdots & & a_n & 0 & 0 & \cdots & & 0 \\
0 & a & a_1 & \cdots & & a_n & 0 & \cdots & & 0 \\
0 & 0 & a & a_1 & \cdots & & a_n & \cdots & & 0 \\
\vdots & & & & & & & & & \\
0 & 0 & \cdots & & & & \cdots & a_{n-2} & a_{n-1} & a_n \\
b & b_1 & \cdots & & & 0 & 0 & \cdots & & 0 \\
0 & b & b_1 & \cdots & & & 0 & \cdots & & 0 \\
0 & 0 & b & b_1 & \cdots & & & \cdots & & 0 \\
\vdots & & & & & & & & & \\
0 & 0 & \cdots & & & & \cdots & b_{m-2} & b_{m-1} & b_m
\end{array}$$

From the above it is easy to deduce the following properties of R:

(4) $$R(G,F)=(-1)^{nm}R(F,G),$$

(5) $$R(F,G_1G_2)=R(F,G_1)R(F,G_2), \qquad R(F_1F_2,G)=R(F_1,G)R(F_2,G),$$

(6) $$R(F,G)=a^{m-\deg(G-FH)}R(F,G-FH) \quad \text{for any } H.$$

The *discriminant* $D(F)$ of a monic polynomial $\prod_{i=1}^n(x-\alpha_i)$ is given by

(7) $$D(F)=\prod_{i<j}(\alpha_i-\alpha_j)^2,$$

which can also be written

(8) $$D(F)=(-1)^{n(n-1)/2}\prod_{i=1}^n F'(\alpha_i),$$

(9) $$D(F)=(-1)^{n(n-1)/2}R(F,F').$$

Our main tool will be Swan's version of Stickelberger's theorem ([1], [3]). Suppose F is a monic polynomial of degree n with integral coefficients and that F, reduced modulo 2 (which we denote by $\bar{F}$ or f), has r irreducible factors. Then

(a) $D(F)\equiv 1 \pmod 8$ implies $r\equiv n \pmod 2$,

(b) $D(F)\equiv 5 \pmod 8$ implies $r\not\equiv n \pmod 2$,

(c) $D(F)\not\equiv 1,5 \pmod 8$ implies f has repeated factors.

Hence, the value of $D(F) \pmod 8$ determines the parity of r if f has no repeated factors and the parity of n is known.

3. Theoretical Results. We consider first a special case. Let g be a polynomial of degree k over the two-element field F_2 with $g(0)=1$, and let G be a polynomial with integer coefficients of the same degree with $\bar{G}=g$. (Take, say, all coefficients of G to be 0 or 1.) Consider the family $\{p_n\}$ of polynomials over F_2 given by $p_n=x^n+g(x)$ and the associated family $\{P_n\}$ with $P_n=x^n+G(x)$. We have (considering only cases with $n>k$)

$$D(P_n)=(-1)^{n(n-1)/2}R(P_n,P_n').$$

However, the assumption $G(0) = 1$ implies $R(P_n, x) = (-1)^n$, so

$$R(P_n, xP_n') = (-1)^n R(P_n, P_n'),$$

and

$$D(P_n) = (-1)^{n(n-1)/2+n} R(P_n, xP_n') = (-1)^{n(n+1)/2} R(P_n, xP_n' - nP_n),$$

using property (6) of Section 2.

Let $H_n = xP_n' - nP_n$, and $h_n = \overline{H}_n$. Then we have $H_n = xG' - nG$ since the contributions from x^n cancel, and $h_n = xg' - ng$ only depends on the parity of n. Hence, if the parity of n is fixed, h_n does not depend on n.

For fixed parity of n, let π denote the period of h_n, i.e., the least positive integer such that h_n divides $x^\pi - 1$ in $F_2[x]$. (If h_n has zero constant term, let π denote the period of k_n where $h_n = x^t k_n$ and $k_n(0) = 1$.) Then we have

THEOREM 1. *Let r_n denote the number of irreducible factors of $p_n = x^n + g$. Then if p_n has no repeated factors (and n is sufficiently large) we have*

$$r_n \equiv r_{n+\mathrm{LCM}(8,4\pi)} \pmod 2,$$

*where π is the period of $h_n = xg' - ng$.**

Proof. Using the Stickelberger-Swan theorem it suffices to prove that

$$D(P_n) \equiv D(P_{n+\mathrm{LCM}(8,4\pi)}) \pmod 8.$$

Now we have shown

$$D(P_n) = (-1)^{n(n+1)/2} R(P_n, H_n)$$

and $(-1)^{n(n+1)/2}$ has period 4, so it suffices to show that $R(P_n, H_n)$ is congruent to

$$R(P_{n+\mathrm{LCM}(8,4\pi)}, H_{n+\mathrm{LCM}(8,4\pi)}) \pmod 8.$$

Clearly H_n and H_{n+8} are congruent (coefficient by coefficient) modulo 8 and have the same degree, so from the determinant definition of the resultant we need only show that

$$R(P_n, H_n) \equiv R(P_{n+4\pi}, H_n) \pmod 8.$$

Since h_n divides $x^\pi - 1$, we know that H_n divides $x^\pi - 1 \pmod 2$, i.e., $x^\pi \equiv 1 + 2K$ (mod H_n). Therefore

$$x^{4\pi} \equiv (1 + 2K)^4 \equiv 1 + 8L \pmod{H_n}.$$

(If h_n divides $x^t(x^\pi - 1)$, then $x^{4\pi+4t} \equiv x^{4t} + 8L$ (mod H_n).)

Case 1. Suppose $n - k$ is odd. Then H_n and h_n have the same degree. This means that in the congruence $x^{4\pi} \equiv 1 + 8L$ (mod H_n) we can take the degree of L to be less than 4π. In other words we have $x^{4\pi} \equiv 1 + H_n M$ (mod 8) with the degree of $1 + H_n M$ equal to 4π. This gives $x^{n+4\pi} \equiv x^n + x^n H_n M$ (mod 8).

Now we have

$$\begin{aligned} R(P_{n+4\pi}, H_n) &= R(x^{n+4\pi} + G, H_n) \\ &\equiv R(x^n + x^n H_n M + G, H_n) \pmod 8, \end{aligned}$$

**Note*: h_n will always be a square or x times a square, so π will be even unless $\pi = 1$, and hence $\mathrm{LCM}(8, 4\pi) = 4\pi$ unless $\pi = 1$.

using the determinant definition of R and the fact that $x^n + x^n H_n M$ has degree $n + 4\pi$. Hence,

$$R(P_{n+4\pi}, H_n) \equiv (k-n)^{4\pi} R(x^n + G, H_n) \pmod 8,$$

where $(k-n)$ is the leading coefficient of H_n and we are using properties (6) and (4) of Section 2. Since $(k-n)^{4\pi} \equiv 1 \pmod 8$ we conclude

$$R(P_{n+4\pi}, H_n) \equiv R(P_n, H_n) \pmod 8.$$

This completes Case 1.

Although we have only given the details when $h_n(0) = 1$, the argument is similar for $t > 0$ and shows that periodicity will hold as soon as n is at least $4t$ (and of course greater than k).

Case 2. Suppose $n - k$ is even. Then h_n has degree $l < k$ and we write $u = k - l$. By applying Hensel's lemma [2, p. 275] we can write $H_n = H_n^{(1)} H_n^{(2)}$, where $H_n^{(1)}$, $H_n^{(2)}$ have 2-adic coefficients

$$\overline{H}_n^{(1)} = h_n, \qquad \overline{H}_n^{(2)} = 1,$$

$H_n^{(1)}$ has degree l, and $H_n^{(2)}$ has degree u. By property (5) of Section 2 we need only that

$$R\left(P_{n+4\pi}, H_n^{(1)}\right) \equiv R\left(P_n, H_n^{(1)}\right) \pmod 8$$

and

$$R\left(P_{n+4\pi}, H_n^{(2)}\right) \equiv R\left(P_n, H_n^{(2)}\right) \pmod 8.$$

The former follows immediately from Case 1. For the latter we proceed as follows. Since $H_n^{(2)} \equiv 1 \pmod 2$ we can write $x \equiv 1 + 2Q \pmod{H_n^{(2)}}$, where the degree of Q is $u + 1$. Hence $x^4 \equiv 1 + 8R \pmod{H_n^{(2)}}$, where the degree of R is $4u + 4$, or $x^4 \equiv 1 + H_n^{(2)} S \pmod 8$ with the degree of $H_n^{(2)} S$ equal to $4u + 4$. Now for any nonzero x^a present in G we have

$$x^{4+a} \equiv x^a + x^a H_n^{(2)} S \pmod 8.$$

Suppose n is larger than $k + 4u$, so that $n + 4$ is larger than $k + 4u + 4$. Then the degree of $x^a H_n^{(2)} S$ will be less than $n + 4$. Hence

$$R\left(x^{n+4} + G, H_n^{(2)}\right) \equiv R\left(x^{n+4} + x^4 G - H_n^{(2)} S G, H_n^{(2)}\right) \pmod 8,$$

using the determinant definition of R. Hence, applying properties (6) and (4) of Section 2, we have

$$R\left(x^{n+4} + G, H_n^{(2)}\right) \equiv R\left(x^{n+4} + x^4 G, H_n^{(2)}\right) \pmod 8.$$

But we have

$$\begin{aligned} R\left(x^4(x^n + G), H_n^{(2)}\right) &= R\left(x^4, H_n^{(2)}\right) R\left(x^n + G, H_n^{(2)}\right) \\ &= \left(H_n^{(2)}(0)\right)^4 R\left(x^n + G, H_n^{(2)}\right) \\ &\equiv R\left(x^n + G, H_n^{(2)}\right) \pmod 8, \end{aligned}$$

using properties (5) and (2) of Section 2. Hence, we have

$$R\left(P_{n+4}, H_n^{(2)}\right) \equiv R\left(P_n, H_n^{(2)}\right) \pmod 8$$

and, upon iterating,

$$R\left(P_{n+4\pi}, H_n^{(2)}\right) \equiv R\left(P_n, H_n^{(2)}\right) \pmod 8.$$

This completes Case 2 and hence the proof of Theorem 1.

In Case 2, periodicity will hold as soon as $n \geqslant 4t$ *and* $n > k + 4u$.

Now let us consider the more general case of a family of polynomials $\{p_n\}$ with $p_n = x^n f + g$, where f, g are *coprime* polynomials over F_2 with $g(0) = f(0) = 1$ (consider only $n > k =$ degree g). Suppose F, G are polynomials with integer coefficients with $\overline{F} = f$, $\overline{G} = g$, degree $F =$ degree f, degree $G =$ degree g. (As before, we take all coefficients of F, G to be 0 or 1.) Let $P_n = x^n F + G$. We have

$$\begin{aligned} R(P_n, P_n') &= R(x^n F + G, nx^{n-1}F + x^n F' + G') \\ &= R(x^n F + G, x)^{-1} R(x^n F + G, nx^n F + x^{n+1}F' + xG') \\ &= (-1)^{n+\deg F} R(x^n F + G, x^{n+1}F' + xG' - nG) \\ &= (-1)^{n+\deg F} R(x^n F + G, F)^{-1} R(x^n F + G, x^{n+1}FF' + xFG' - nFG) \\ &= (-1)^{n+\deg F} R(G, F)^{-1} R(x^n F + G, xFG' - xGF' - nFG), \end{aligned}$$

using various properties from Section 2. Letting $H_n = xFG' - xF'G - nFG$, and hence obtaining

$$h_n = \overline{H}_n = xfg' - xf'g - nfg = f^2\big(x(g/f)' - n(g/f)\big),$$

we have

THEOREM 2. *Let r_n denote the number of irreducible factors of $p_n = x^n f + g$. If p_n has no repeated factors (and n is sufficiently large), then* $r_n \equiv r_{n+\mathrm{LCM}(8,4\pi)} \pmod 2$, *where π is the period of $h_n = f^2(x(g/f)' - n(g/f))$.***

From the above calculations it clearly suffices (for the proof of Theorem 2) to show that

$$R(P_n, H_n) \equiv R(P_{n+4\pi}, H_n) \pmod 8.$$

We omit the details, since they are very similar to those of the proof of Theorem 1, i.e., the case $f = 1$. Periodicity will again hold as soon as $n \geqslant 4t$ and $n > k + 4u$, where x^t exactly divides h_n, $k =$ degree g, and $u =$ degree $H_n -$ degree h_n.

4. Further Comments. Although our results appear to be best possible in general, there are many special cases in which the actual period of the function r_n is less than the period predicted by our theorems. One such case is that of trinomials $x^n + x^k + 1$ with n odd and k even, where the period is 8 rather than $4k$.

Theorems 1 and 2 do not address the case of repeated factors. Certainly, if p_n has repeated factors so will $p_{n+\mathrm{LCM}(8,4\pi)}$, since this is detected by the parity of $D(P_n)$. Unfortunately, the Stickelberger-Swan theorem does not give information about the parity of r_n in this case. However, any repeated factors of p_n must divide h_n. For given h_n these can be divided out of p_n at the start, giving a new family of polynomials parameterized by n in a more complicated way than that of our Theorems 1 and 2. Our techniques can be used to extend our results to cover this situation also, and hence to extend Theorems 1 and 2 to the repeated factor case. We omit the (relatively messy) details.

Finally, consider a family of the form $p_n = x^n + g(x)$, where n is odd and $g(x) = u(x)^2$. Then $h_n = g$. Suppose further that $u(x)$ has odd period π'. Then $u(x)$ and $(x^{\pi'} - 1)/u(x)$ are coprime, so we can find (by Hensel's lemma) 2-adic

***Note*: As in Theorem 1, either $\mathrm{LCM}(8, 4\pi) = 4\pi$ or $\pi = 1$.

polynomials $U(x)$, $V(x)$ with $\overline{U} = u$, $UV = x^{\pi'} - 1$, and degree U = degree u. This gives $x^{2\pi'} - 1 = U(x^2)V(x^2)$, where $\overline{U}(x^2) = u(x)^2 = g(x)$. By appropriately choosing G (i.e., no longer with 0, 1 coefficients) with degree G = degree g, $\overline{G} = g$, we can guarantee that $H_n = xG' - nG$ is congruent to $U(x^2)$ (mod 8). (Adding two to the coefficient of a term x^a of G adds $2(a-n)$ to the coefficients of x^a in H_n.) Hence $x^{2\pi'} \equiv 1 + H_n M$ (mod 8). From this, as in Case 1 of Theorem 1, we deduce

$$R(P_{n+4\pi'}, H_n) \equiv R(P_n, H_n) \pmod 8.$$

On the other hand, if we compare $R(P_{n+4\pi'}, H_n)$ and $R(P_{n+4\pi'}, H_{n+4\pi'})$ via the determinant definition of R, using the fact that the nonzero coefficients of $H_{n+4\pi'}$ are each $4\pi'$ smaller than those of H_n, and the fact that for any odd integer N we have $N - 4 \equiv (-3)N$ (mod 8), we find that

$$R(P_{n+4\pi'}, H_{n+4\pi'}) \equiv (-3)^{\pi'(n+4\pi')} R(P_{n+4\pi'}, H_n) \pmod 8.$$

But $(-3)^{\pi' n} \equiv (-3)$ (mod 8), so we conclude that r_n *is antiperiodic with antiperiod* $4\pi'$. (Note that the predicted *period* of r_n is $4\pi = 8\pi'$, which this result implies.)

5. Experimental Results. In this section, we give tables of values of r_n for various f, g, and n. The cases where Theorem 1 applies ($f = 1$) are listed first. The cases of odd and even n are listed separately. The parity (0 or 1) of r_n is also given.

After each table, we give the polynomial $h = h_n$; the predicted period LCM$(8, 4\pi)$ of r_n; the observed period (if it is different); and the antiperiod for those cases covered in Section 4.

I. $f = 1$; $g = x^3 + x + 1$.

n	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34
r_n	3	4	3	5	3	4	5	5	5	6	3	5	5	4	3	7
parity	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1	1

$h = x^3 + x$; period = 8.

II. $f = 1$; $g = x^4 + x^2 + 1$.

n	5	7	9	11	13	15	17	19	21	23	25	27	29	31
r_n	2	2	2	2	3	4	3	3	3	3	2	3	4	4
parity	0	0	0	0	1	0	1	1	1	1	0	1	0	0

n	33	35	37	39	41	43	45	47	49	51	53	55	57	59
r_n	2	4	3	2	3	5	3	5	2	5	4	2	4	4
parity	0	0	1	0	1	1	1	1	0	1	0	0	0	0

$h = x^4 + x^2 + 1$; period = 24; antiperiod = 12.

III. $f = 1$; $g = x^5 + x + 1$.

n	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36
r_n	3	5	3	6	4	7	4	6	3	5	5	6	6	5	4	8
parity	1	1	1	0	0	1	0	0	1	1	1	0	0	1	0	0

$h = x^5 + x$; period = 16.

IV. $f = 1$; $g = x^6 + x^2 + 1$.

n	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37
r_n	2	2	3	2	2	3	4	3	4	4	2	5	3	5	5	5
parity	0	0	1	0	0	1	0	1	0	0	0	1	1	1	1	1

n	39	41	43	45	47	49	51	53	55	57	59	61	63
r_n	4	3	5	2	5	4	5	5	3	4	6	4	4
parity	0	1	1	0	1	0	1	1	1	0	0	0	0

$h = x^6 + x^2 + 1$; period = 56; antiperiod = 28.

V. $f = 1$; $g = x^7 + x + 1$.

n	8	10	12	14	16	18	20	22	24	26	28	30
r_n	4	4	5	4	3	7	4	7	6	5	3	6
parity	0	0	1	0	1	1	0	1	0	1	1	0

n	32	34	36	38	40	42	44	46	48	50	52	54
r_n	4	4	7	4	3	9	4	5	6	7	5	8
parity	0	0	1	0	1	1	0	1	0	1	1	0

$h = x^7 + x$; period $= 24$.

VI. $f = 1$; $g = x^8 + x^4 + 1$.

n	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45
r_n	3	2	4	3	3	2	2	3	3	4	2	3	3	2	4	3	5	4	4
parity	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0

$h = x^8 + x^4 + 1$; predicted period $= 48$; observed period $= 8$.

VII. $f = 1$; $g = x^9 + x + 1$.

n	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40
r_n	4	6	4	10	4	6	4	10	5	8	5	10	5	6	5	12
parity	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0

n	42	44	46	48	50	52	54	56	58	60	62	64	66	68	70	72
r_n	4	6	6	10	4	8	4	12	7	6	3	12	5	6	7	12
parity	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0

$h = x^9 + x$; period $= 32$.

VIII. $f = 1$; $g = x^9 + x + 1$.

n	11	13	15	17	19	21	23	25	27	29	31	33
r_n	3	4	2	3	5	4	3	5	3	4	5	3
parity	1	0	0	1	1	0	1	1	1	0	1	1

n	35	37	39	41	43	45	47	49	51	53	55	57
r_n	2	4	5	3	6	4	5	5	4	4	5	2
parity	0	0	1	1	0	0	1	1	0	0	1	1

$h = 1$; period $= 8$.

IX. $f = 1$; $g = x^{17} + x + 1$.

n	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48
r_n	4	6	4	10	3	6	4	18	6	6	5	12	4	6	4	20
parity	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0

n	50	52	54	56	58	60	62	64	66	68	70	72	74	76	78	80
r_n	5	8	3	10	4	6	7	18	5	6	4	10	5	6	3	20
parity	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0

$h = x^{17} + x$; period $= 64$.

X. $f = 1$; $g = x^5 + x^3 + x + 1$.

n	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36
r_n	3	1	2	4	1	1	4	2	1	5	2	2	5	3	2	4
parity	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0

n	38	40	42	44	46	48	50	52	54	56	58	60	62
r_n	3	3	6	2	3	5	2	4	7	3	4	4	3
parity	1	1	0	0	1	1	0	0	1	1	0	0	1

$h = x^5 + x^3 + x$; predicted period $= 24$; observed period $= 8$.

XI. $f = 1;\ g = x^7 + x^3 + x + 1.$

n	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39
r_n	2	2	1	3	2	2	3	1	3	2	4	1	3	4	2	3
parity	0	0	1	1	0	0	1	1	1	0	0	1	1	0	0	1

n	41	43	45	47	49	51	53	55	57	59
r_n	1	2	2	1	3	2	4	3	3	4
parity	1	0	0	1	1	0	0	1	1	0

$h = 1$; period $= 8$.

XII. $f = 1;\ g = x^7 + x^3 + x + 1.$

n	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36
r_n	1	1	1	4	2	2	2	1	3	3	4	1	3	3	2
parity	1	1	1	0	0	0	0	1	1	1	0	1	1	1	0

n	38	40	42	44	46	48	50	52	54	56	58	60	62	64	66	68	70
r_n	2	4	3	5	5	3	2	2	4	6	2	4	2	3	3	3	4
parity	0	0	1	1	1	1	0	0	0	0	0	0	0	1	1	1	0

n	72	74	76	78	80	82	84	86	88	90	92	94	96	98	100	102	104
r_n	4	4	2	3	3	3	8	3	3	3	4	2	4	3	3	5	5
parity	0	0	0	1	1	1	0	1	1	1	0	0	0	1	1	1	1

$h = x^7 + x^3 + x$; period $= 56$.

XIII. $f = 1;\ g = x^8 + x^7 + x + 1.$

n	10	12	14	16	18	20	22	24	26	28	30	32
r_n	4	1	2	3	3	1	4	2	1	4	2	2
parity	0	1	0	1	1	1	0	0	1	0	0	0

n	34	36	38	40	42	44	46	48	50	52	54	56	58	60
r_n	7	1	2	7	3	3	4	2	3	6	2	4	7	5
parity	1	1	0	1	1	1	0	0	1	0	0	0	1	1

$h = x^7 + x$; period $= 24$.

XIV. $f = 1;\ g = x^9 + x^5 + x + 1.$

n	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48
r_n	1	5	2	2	3	1	1	6	2	1	4	2	1	5	2	2	4	3	3	6
parity	1	1	0	0	1	1	1	0	0	1	0	0	1	1	0	0	0	1	1	0

n	50	52	54	56	58	60	62	64	66	68	70	72	74	76	78	80	82	84	86	88
r_n	2	3	5	4	5	7	2	2	5	3	3	8	2	3	6	2	3	7	4	2
parity	0	1	1	0	1	1	0	0	1	1	1	0	0	1	0	0	1	1	0	0

$h = x^9 + x^5 + x$; period $= 48$.

XV. $f = x + 1;\ g = x^2 + x + 1.$

n	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
r_n	1	1	1	2	1	3	2	2	1	3	4	2	3	1	2	2
parity	1	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0

n	35	37	39	41	43	45	47	49
r_n	3	3	2	4	3	3	2	2
parity	1	1	0	0	1	1	0	0

$h = 1$; period $= 8$.

XVI. $f = x + 1$; $g = x^2 + x + 1$.

n	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34
r_n	1	2	2	2	1	1	2	2	3	1	2	2	3	3	2	2
parity	1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0

n	36	38	40	42	44	46	48
r_n	3	3	2	2	3	3	4
parity	1	1	0	0	1	1	0

$h = x^3$; period = 8.

XVII. $f = x + 1$; $g = x^3 + x + 1$.

n	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38
r_n	1	1	3	1	2	2	1	3	2	2	3	3	2	2	3	3	2	4
parity	1	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0

$h = x^3$; period = 8.

XVIII. $f = x + 1$; $g = x^3 + x + 1$.

n	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
r_n	3	1	2	3	1	2	4	2	1	5	2	3	7	1	4
parity	1	1	0	1	1	0	0	0	1	1	0	1	1	1	0

n	35	37	39	41	43	45	47	49	51	53	55
r_n	5	1	2	4	4	3	5	2	1	5	1
parity	1	1	0	0	0	1	1	0	1	1	1

$h = x^4 + x^2 + 1$; period = 24.

XIX. $f = x + 1$; $g = x^3 + x^2 + 1$.

n	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34
r_n	1	2	2	1	2	2	1	3	2	2	5	1	2	2	3	1
parity	1	0	0	1	0	0	1	1	0	0	1	1	0	0	1	1

n	36	38	40	42	44	46	48	50
r_n	4	2	1	5	2	2	3	3
parity	0	0	1	1	0	0	1	1

$h = x$; period = 8.

XX. $f = x + 1$; $g = x^3 + x^2 + 1$.

n	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
r_n	1	1	4	1	1	4	2	2	5	2	2	4	5	1	4
parity	1	1	0	1	1	0	0	0	1	0	0	0	1	1	0

n	35	37	39	41	43	45	47	49	51
r_n	3	3	4	2	2	5	2	2	4
parity	1	1	0	0	0	1	0	0	0

$h = x^4 + x^2 + 1$; period = 24.

XXI. $f = x + 1$; $g = x^4 + x^2 + 1$.

n	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
r_n	1	2	1	2	1	1	3	3	2	3	2	4	2	4	1
parity	1	0	1	0	1	1	1	1	0	1	0	0	0	0	1

n	35	37	39	41	43	45	47	49	51
r_n	4	3	1	3	1	4	5	4	2
parity	0	1	1	1	1	0	1	0	0

$h = x^4 + x^2 + 1$; period = 24.

XXII. $f = x + 1$; $g = x^4 + x^2 + 1$.

n	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34
r_n	1	1	2	1	2	2	2	2	1	2	3	3	1	3	2
parity	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0

n	36	38	40	42	44	46	48	50
r_n	1	4	2	4	2	5	4	1
parity	1	0	0	0	0	1	0	1

$h = x^5 + x^3 + x$; period $= 24$.

XXIII. $f = x^2 + 1$; $g = x^4 + x^2 + 1$.

n	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
r_n	2	1	1	3	1	2	3	2	2	2	4	3	2	3	3
parity	0	1	1	1	1	0	1	0	0	0	0	1	0	1	1

n	35	37	39	41	43	45	47	49	51
r_n	3	1	4	3	2	2	4	2	3
parity	1	1	0	1	0	0	0	0	1

$h = x^6 + 1$; period $= 24$.

XXIV. $f = x^2 + x + 1$; $g = x^3 + x + 1$.

n	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34
r_n	2	2	2	3	3	3	4	2	3	3	2	2	3	5	4	2
parity	0	0	0	1	1	1	0	0	1	1	0	0	1	1	0	0

n	36	38	40	42	44	46	48	50
r_n	5	5	4	4	5	5	2	4
parity	1	1	0	0	1	1	0	0

$h = x^5$; period $= 8$.

XXV. $f = x^2 + x + 1$; $g = x^3 + x + 1$.

n	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
r_n	3	5	4	6	4	5	3	6	3	7	4	8	4	7	5
parity	1	1	0	0	0	1	1	0	1	1	0	0	0	1	1

n	35	37	39	41	43	45	47	49	51
r_n	5	5	7	4	8	6	7	5	8
parity	1	1	1	0	0	0	1	1	0

$h = x^4 + 1$; period $= 16$.

XXVI. $f = x^2 + x + 1$; $g = x^3 + x^2 + 1$.

n	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34
r_n	3	6	3	5	4	6	4	7	5	8	3	7	4	6	4	9
parity	1	0	1	1	0	0	0	1	1	0	1	1	0	0	0	1

n	36	38	40	42	44	46	48	50
r_n	3	6	3	7	4	8	6	7
parity	1	0	1	1	0	0	0	1

$h = x^5 + x$; period $= 16$.

XXVII. $f = x^2 + x + 1$; $g = x^3 + x^2 + 1$.

n	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
r_n	2	2	2	2	3	2	2	3	3	2	4	5	3	4	4
parity	0	0	0	0	1	0	0	1	1	0	0	1	1	0	0

n	35	37	39	41	43	45	47	49	51
r_n	3	3	2	4	3	3	4	4	3
parity	1	1	0	0	1	1	0	0	1

$h = 1$; period $= 8$.

XXVIII. $f = x^3 + x^2 + 1$; $g = x^3 + x + 1$.

n	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38
r_n	5	3	2	4	3	3	6	4	5	5	6	2	5	3	2	6
parity	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0

$h = x^5 + x^3 + x$; predicted period $= 24$; observed period $= 8$.

XXIX. $f = x^3 + x^2 + 1$; $g = x^3 + x + 1$.

n	9	11	13	15	17	19	21	23	25	27	29	31	33
r_n	6	5	8	3	6	5	7	7	6	3	8	5	6
parity	0	1	0	1	0	1	1	1	0	1	0	1	0

n	35	37	39	41	43	45	47	49	51	53	55
r_n	7	7	7	8	5	8	7	8	5	9	5
parity	1	1	1	0	1	0	1	0	1	1	1

$h = x^6 + x^4 + x^2 + 1$; predicted period $= 32$; observed period $= 16$.

Department of Mathematics
Naval Postgraduate School
Monterey, California 93943

Department of Mathematics
University of California, Los Angeles
Los Angeles, California 90024

The Aerospace Corporation
P. O. Box 92957
Los Angeles, California 90009

1. E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

2. Z. I. Borevich & I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

3. R. G. Swan, "Factorization of polynomials over finite fields," *Pacific J. Math.*, v. 12, 1962, pp. 1099–1106.