Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Jacob T.B. jun. Beard, James R. jun. O'Connell, Karen I. West

Perfect polynomials over GF(q)

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **62** (1977), n.3, p. 283–291.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1977_8_62_3_283_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1977.

Algebra. — *Perfect polynomials over* GF (q) (*). Nota di JACOB T. B. BEARD, JR., JAMES R. OCONNELL, JR. e KAREN I. WEST, presentata (**) dal Socio B. SEGRE.

RIASSUNTO. — Un polinomio monico $A(x) \in GF[q, x]$ dicesi *perfetto* su GF (q) se, e soltanto se, $A(x)$ uguaglia la somma $\sigma(A(x))$ dei divisori monici distinti di $A(x)$ in GF $[q, x]$. Si caratterizzano i polinomi perfetti su GF (q) che sono riducibili in GF $[p, x]$, e si formulano congetture analoghe a quelle classiche sui numeri perfetti dispari.

1. INTRODUCTION AND NOTATION

E. F. Canaday, the first doctoral student of L. Carlitz, considered in 1941 [1] the sum $\sigma(A(x))$ of the distinct divisors of the polynomial $A(x) \in GF[2, x]$. We generalize the domain of σ and define $\sigma(A(x))$ as the sum of the distinct monic divisors in GF $[q, x]$ of the monic polynomial $A(x) \in GF[q, x]$, $q = p^d$, $d \geq 1$. In the case $A(x) = \sigma(A(x))$, we call the polynomial $A(x) \in GF[q, x]$ *perfect* over GF (q). The purpose of this paper is to continue and extend the basic study begun by OConnell [2]. The principal result is a characterization of all perfect polynomials over GF (p) which split in GF $[p, x]$. Related results (§ 3) lead to conjectural analogs of the classical question on the existence of odd perfect numbers, and we display (§ 4) all currently known perfect polynomials over GF (q) which do not split in GF $[q, x]$, $q = 2, 3, 5$. We are indebted to L. I. Wade, the second doctoral student of Carlitz, for introducing us to the work of Canaday, and to both Professors Carlitz and Wade for their enthusiasm toward our efforts.

Throughout this paper, we are led by only two of Canaday's several results. First, that $x^\alpha (x-1)^\beta$ is perfect over GF (2) if and only if $\alpha = \beta = 2^n - 1$ for some $n \geq 0$ and, second, that whenever $A(x)$ is perfect over GF (2), then either $x(x-1) \mid A(x)$ or else $(x(x-1), A(x)) = 1$ and A is a perfect square. Canaday found it " plausible " that no perfect polynomials of the last type exist, hence the conjecture in § 3 is not original with us.

Monic polynomials over GF (q) are denoted $A, B, C, \cdots$, while prime (monic irreducible) polynomials over GF (q) are denoted $P, Q, R, \cdots$. Following Canaday, we write $A \to B$ whenever $\sigma(A) = B$. It is clear that $\deg A = \deg \sigma(A)$ and that $\sigma(AB) = \sigma(A)\sigma(B)$ whenever $(A, B) = 1$.

(*) This research was partially supported by an Organized Research Grant from The University of Texas at Arlington.

(**) Nella seduta del 12 marzo 1977.

Thus whenever $A \in GF[q, x]$ has the canonical decomposition $A = \prod_{i=1}^{n} P_i^{\alpha(i)}$ as the product of powers of distinct primes P_i with $\alpha(i) > 0$, then

$$A = \prod_{i=1}^{n} P_i^{\alpha(i)} \to \prod_{i=1}^{n} \sigma(P_i^{\alpha(i)}) = \prod_{i=1}^{n} \sum_{j=0}^{\alpha(i)} P_i^j .$$

This fact, that σ is multiplicative on its domain, is used extensively and without further reference, as is the basic identity

$$\sum_{j=0}^{\alpha(i)} P_i^j = (P_i^{\alpha(i)+1} - 1)/(P_i - 1) .$$

Though transparent, the following result is very useful—either in showing a polynomial to be perfect, or in showing a polynomial not to be perfect.

LEMMA. *The polynomial* A *is perfect over* GF (q) *if and only if for each prime polynomial* $P \in GF[q, x]$, $m = n$ *whenever* $P^m \| A$ *and* $P^n \| \sigma(A)$.

As usual, $P^k \| B$ is equivalent to $P^k \mid B$ and $P^{k+1} \nmid B$.

2. PERFECT SPLITTING POLYNOMIALS

In Theorem 8, § 3, we will show that whenever the polynomial A is perfect over GF (p) and $(x - i) \mid A$ for some i, $0 \leq i < p$, then $\prod_{i=0}^{p-1} (x - i) \mid A$. (As usual, we take the integers *modulo* p as our representation for GF (p)). Thus in characterizing all perfect polynomials A which split in $GF[p, x]$, it suffices to consider

$$A = \prod_{i=0}^{p-1} (x - i)^{\alpha(i)}, \qquad \alpha(i) > 0 .$$

The analogous statement for $A \in GF[q, x]$ does not hold, by a later example. For this and other reasons, we obtain only a partial characterization for perfect polynomials which split in $GF[q, x]$. We first assume $\alpha(i) = k > 0$ for $0 \leq i < p$ and determine all integers k such that $A = \prod_{i=0}^{p-1} (x - 1)^k$ is perfect. As a guide through our strategy, recall that any positive integer k can be uniquely represented to the base p as $k = \sum_{i=1}^{n} k(i)\, p^i - k(0)$, where $0 \leq k(i) < p$ for $0 \leq i \leq n$.

THEOREM 1. *The polynomial* $A = \prod_{a \in GF(q)} (x - a)^{p^n - 1}$ *is perfect over* GF (q) *for each* $n \geq 0$.

Proof. For each $a \in \mathrm{GF}(q)$,

$$(x - a)^{p^n - 1} \to \frac{(x - a)^{p^n} - 1}{x - a - 1} = \frac{(x - a - 1)^{p^n}}{x - a - 1} = (x - a - 1)^{p^n - 1},$$

so that

$$\mathrm{A} = \prod_a (x - a)^{p^n - 1} \to \prod_a (x - a - 1)^{p^n - 1} = \mathrm{A}.$$

THEOREM 2. *The polynomial* $\mathrm{A} = \prod_{a \in \mathrm{GF}(q)} (x - a)^{\mathrm{N}p^n - 1}$ *is perfect over* GF (q) *whenever* $\mathrm{N} \mid (q - 1)$, $\mathrm{N} \neq 1$, *and* $n \geq 0$.

Proof. Note that $y^{\mathrm{N}} - 1 = \prod_{b \in \mathrm{H}} (y - b)$ where H is the unique (multiplicative) subgroup of GF $(q)^*$ of order N. Thus for each $n \geq 0$, each admitted N, and for any fixed $a \in \mathrm{GF}(q)$, we have

$$(x - a)^{\mathrm{N}p^n - 1} \to \frac{[(x - a)^{\mathrm{N}} - 1]^{p^n}}{x - a - 1} = (x - a - 1)^{p^n - 1} \prod_{\substack{b \in \mathrm{H} \\ b \neq 1}} (x - a - b)^{p^n}.$$

Hence $(x - a)$ is contributed to $\sigma(\mathrm{A})$ only by

$$(x - a + 1)^{\mathrm{N}p^n - 1} \to (x - a)^{p^n - 1} \prod_{\substack{b \in \mathrm{H} \\ b \neq 1}} (x - a + 1 - b)^{p^n}$$

and, for each $b \in \mathrm{H} - \{1\}$,

$$(x - a + b)^{\mathrm{N}p^n - 1} \to (x - a + b - 1)^{p^n - 1} (x - a)^{p^n} \prod_{\substack{c \in \mathrm{H} \\ 1 \neq c \neq b}} (x - a + b - c)^{p^n}.$$

Since there are precisely $(\mathrm{N} - 1)$ such $b \in \mathrm{H} - \{1\}$, then $(x - a)^{\mathrm{N}p^n - 1} \parallel \sigma(\mathrm{A})$ as $(p^n - 1) + (\mathrm{N} - 1) p^n = \mathrm{N}p^n - 1$, and we are done by the Lemma.

It is convenient hereafter to treat the cases $\mathrm{N} = 1$ and $\mathrm{N} > 1$ simultaneously and adopt the convention that indexed products over the empty set take the value of 1. From Theorem 1 and Theorem 2 we have the sufficiency of

THEOREM 3. *The polynomial* $\mathrm{A} = \prod_{a \in \mathrm{GF}(q)} (x - a)^{\mathrm{N}p^n - 1}$ *is perfect over* GF (q) *if and only if* $\mathrm{N} \mid (q - 1)$ *and* $n \geq 0$.

Proof. We prove the necessity by contraposition. Without loss of generality assume $(\mathrm{N}, p) = 1$, and $\mathrm{N} \nmid (q - 1)$. Consider

$$x^{\mathrm{N}p^n - 1} \to \frac{(x^{\mathrm{N}} - 1)^{p^n}}{x - 1}.$$

Since $p \nmid \mathrm{N}$, then $(x^{\mathrm{N}} - 1) \notin \mathrm{GF}[q, x^p]$, so that $x^{\mathrm{N}} - 1$ has no repeated roots in GF (q). Furthermore, $x^{\mathrm{N}} - 1$ has precisely $(\mathrm{N}, q - 1)$ distinct roots in GF (q), and $(\mathrm{N}, q - 1) < \mathrm{N}$. Hence $x^{\mathrm{N}} - 1$ does not split in GF $[q, x]$ and, by the Lemma, the polynomial A is not perfect.

In the case $q = p$, we obtain a stronger result.

THEOREM 4. *The polynomial* $A = \prod_{i=0}^{p-1} (x - i)^k$ *is perfect over* GF (p) *if and only if* $k = Np^n - 1$ *where* $N \mid (p - 1)$ *and* $n \geq 0$.

Proof. There remains only to prove the necessity in the case $k \geq p$ and $k \neq Np^n - 1$. For this case, let $k = \sum_{j=1}^{m} k(j)\, p^j - k(0)$ where $0 \leq k(j) < p$ for $0 \leq j < m$ and $0 < k(m) < p$, and consider

$$x^k \to \frac{x^{k(m)p^m + \cdots + k(1)p - k(0) + 1} - 1}{x - 1} = \frac{B}{x - 1}.$$

Again, it suffices to show that the polynomial B does not split in GF $[p, x]$. If $k(0) \neq 1$, this is easily seen since $B \notin \mathrm{GF}[p, x^p]$ and $\deg B = k + 1 > p$. If $k(0) = 1$, then

$$B = (x^{k(m)p^{m-l} + \cdots + k(l)} - 1)^{p^l} = B_1^{p^l}$$

where l is the least positive integer j such that $k(j) \neq 0$. Then $B_1 \notin \mathrm{GF}[p, x^p]$ and $\deg B_1 > p$. Hence B_1 does not split in GF $[p, x]$, neither does the polynomial B, and the proof is complete.

The perfect splitting polynomials in GF $[p, x]$ are fully characterized in

THEOREM 5. *The polynomial* $A = \prod_{i=0}^{p-1} (x - i)^{\alpha(i)}$ *is perfect over* GF (p) *if and only if* $\alpha(0) = \alpha(j)$ *for* $1 \leq j < p$ *and* $\alpha(0) = Np^n - 1$ *for some* $N \mid (p - 1)$ *and some* $n \geq 0$.

Proof. If some $\alpha(i)$ is not of the form $Np^n - 1$ with $N \mid (p - 1)$ and $n \geq 0$ then $\sigma((x - i)^{\alpha(i)})$ does not split in GF $[p, x]$ for this i, as argued in proving Theorem 3 and Theorem 4, and hence A is not perfect. By Theorem 4, there remains only to establish the necessity of the equality of the exponents $\alpha(i)$ $0 \leq i < p$. For $0 \leq i < p$, let $\alpha(i) = N(i)\, p^{n(i)} - 1$ where $N(i) \mid (p - 1)$ and $n(i) \geq 0$. As in the proof of Theorem 2, for each fixed j, $0 \leq j < p$,

$$(2.1) \qquad (x - j)^{N(j)p^{n(j)} - 1} \to (x - j - 1)^{p^{n(j)} - 1} \prod_{\substack{a \in H_j \\ a \neq 1}} (x - j - a)^{p^{n(j)}}$$

If A is perfect, it follows from (2.1) and the Lemma that $n(j + 1) = n(j)$ for $0 \leq j < p$. Thus for $0 \leq i < p$, $\alpha(i) = N(i)\, p^n - 1$ for some $n \geq 0$. From (2.1), all $(x - j)$ contributions to $\sigma(A)$ arise from

$$(2.2) \qquad (x - j + 1)^{N(j-1)p^n - 1} \to (x - j)^{p^n - 1} \prod_{\substack{a \in H_{j-1} \\ a \neq 1}} (x - j + 1 - a)^{p^n},$$

or else $b \in H_{j-b} - \{1\}$ and

$$(2.3) \quad (x - j + b)^{N(j-b)p^n - 1} \to (x - j + b - 1)^{p^n - 1} (x - j)^{p^n} \prod_{\substack{c \in H_{j-b} \\ 1 \neq c \neq b}} (x - j + b - c)^{p^n}.$$

If the polynomial A is perfect, then precisely $N(j) - 1$ contributions $(x-j)^{p^n}$ must be realized in the manner of (2.3). Hence there exist precisely $N(j)$ elements $b \in GF(p)$ such that $b \in H_{j-b}$. For the remaining $p - N(j)$ elements $d \in GF(p)$, we must have $d \notin H_{j-d}$. Since j is arbitrary, it follows that $N(i) = N(j)$ for $0 \leq i, j < p$.

3. RELATED RESULTS

Our remaining results lead us to state the

CONJECTURE. *If the polynomial* A *is perfect over* GF (p), *then* $x \mid A$. *More generally, if* A *is perfect over* GF (q), *then* $(x-a) \mid A$ *for some* $a \in GF(q)$.

The generalization of the initial statement of the Conjecture to GF (q) is false. Let $q = p^d$, $d > 1$, and choose any fixed $a \in GF(q)$ with $a \notin GF(p)$. For the polynomial $A = \prod_{i=0}^{p-1} (x - a - i)$, we have $(x - a - i) \to (x - a - i + 1)$ so that A is perfect, and $x \nmid A$. Though not proved, we suspect from Theorem 7 that linear polynomials which divide perfect polynomials over GF (q) do so simultaneously as members of p-rings [1]. Analogous to continuing attacks on the existence of odd perfect numbers, we have

THEOREM 6. *A minimum of* p *distinct prime polynomials divide each polynomial which is perfect over* GF (q).

Proof. Let the polynomial $A = \prod_{i=1}^{n} P_i^{n(i)}$ where the primes $P_i \in GF[q, x]$ are distinct, $n(i) > 0$, and suppose $n < p$. For each j such that $\deg P_j = \min_i \{\deg P_i\}$ let

$$A_j = P_j^{n(j)-1} \prod_{i \neq j} P_i^{n(i)}.$$

Then $\deg A_j = \sum_{i=0}^{n} \deg P_i^{n(i)} - \deg P_j$ is the maximum degree of all admissible summands of $\sigma(A) - A$. The number m of such summands A_j satisfies $1 \leq m \leq n < p$ and each A_j is monic. Hence $\sum_{i=1}^{m} A_j \neq 0$, $\sigma(A) - A \neq 0$, A is not perfect, and we are done by contraposition.

COROLLARY. *The polynomial* $A = \prod_{i=0}^{p-1} (x - i)$ *is the unique perfect polynomial over* GF (p) *of degree* p.

The proof of Theorem 6 generalizes directly to yield the following two results.

THEOREM 7. *If the polynomial* $A = \prod_{i=1}^{n} P_i^{\alpha(i)}$ *is perfect over* GF (q), *the primes* $P_i \in GF[q, x]$ *are distinct,* $\alpha(i) > 0$, *and* $\deg P_1 \leq \deg P_2 \leq \cdots \leq \deg P_n$, *then for some integer* $k \geq 1$, $\deg P_1 = \deg P_j$ *for each* j *satisfying* $1 \leq j \leq kp$.

THEOREM 8. *Let the polynomial* $A \in GF[p, x]$ *be perfect. If* $(x - i) \mid A$ *for some* i, $0 \leq i \leq p$, *then* $\prod_{i=0}^{p-1} (x - i) \mid A$.

In the case $p = 2$, our concluding result coincides with the second mentioned result of Canaday [1; Theorem 1].

THEOREM 9. *Let the polynomial* $A = \prod_{i=1}^{k} P_i^{n(i)}$ *be perfect over* $GF(p)$ *where* $n(i) > 0$ *and the distinct primes* P_i *have constant terms* c_i *respectively. Then* $x \mid A$ *unless all of the following are satisfied*:

i) $\left(\prod_{j=0}^{p-1} (x - j), A\right) = 1$,

ii) $n(i) \equiv 0 \pmod 2$ *whenever* $c_i = p - 1$,

iii) $n(i) \not\equiv -1 \pmod p$ *whenever* $c_i = 1$,

iv) $n(i) \not\equiv -2 \pmod{p-1}$ *whenever* $1 < c_i < p - 1$.

Proof. Condition i) holds by Theorem 8. To see ii)-iv), let

$$A = \sigma(A) = \prod_{i=1}^{k} \sum_{m=0}^{n(i)} P_i^m$$

so that the polynomial A has constant term c given by

$$c = \prod_{i=1}^{k} \sum_{m=0}^{n(i)} c_i^m.$$

If $x \nmid A$ then $c \neq 0$, so that ii) and iii) hold immediately. It follows from Euler's Theorem that $\sum_{m=0}^{p-2} a^m \equiv 0 \pmod p$ whenever $1 < a < p$, from which iv) is immediate.

4. SOME NON-SPLITTING PERFECT POLYNOMIALS

The perfect polynomials given in this section over GF(3) and GF(5) were constructed by OConnell [2], based on factorization tables and sum of divisors tables obtained by Beard and West (unpublished). The latter tables give $\sigma(A)$ for all monic polynomials $A \in GF(p)$ not divisible by x and of degree n as follows:

$$p = 2, 2 \leq n \leq 15 \quad ; \quad p = 3, 2 \leq n \leq 9 \quad ; \quad p = 5, 2 \leq n \leq 6.$$

For monic polynomials A not divisible by x, we have determined (on an IBM 360/155) all perfect polynomials over $GF(p)$ of the form $x^k A$ where $0 \leq k \leq \deg A \leq 15\ (p = 2), 9\ (p = 3), 6\ (p = 5)$. Those over GF(2) which do not split are ten of the eleven " non-trivial " one-rings given by Canaday [1], who asserted them likely to be the only ones of this type. The question

remains open. For completeness, we include these eleven perfect polynomials of Canaday in Table I so that all known non-splitting perfect polynomialls over GF(p) are listed for $p = 2, 3, 5$. Each polynomial is displayed by its prime-power factorization. We observe interesting generating expressions for certain groups of these polynomials and, unfortunately, that none of them appear to generalize. Let σ^k denote the k-fold composite of σ with itself and let y vary as $y = x - i$, $0 \leq i < p$. For $p = 3$, the (three) given polynomials of degree 8 are all generated by each of the products $y^3\,\sigma(y)\,\sigma^2(y)\,\sigma(y^3)$ and $\sigma^4(y^3)\,\sigma(y)\,\sigma^2(y)\,\sigma(y^3)$; those of degree 16 are generated by $y^3\,\sigma(y)\,\sigma(y^4)\,\sigma^2(y^4)\,\sigma^3(y^4)$; those of degree 23 by $y^4\,\sigma(y)\,\sigma^2(y)\,\sigma^3(y)\,\sigma^4(y)\,\sigma^5(y)\,\sigma^6(y)\,\sigma(y^7)\,\sigma^2(y^7)$; and those of degree 28 are generated by $y^5\,\sigma(y)\,\sigma^2(y)\,\sigma(y^2)\,\sigma(y^6)\,\sigma^2(y^6)\,\sigma^3(y^6)$.

TABLE I

Non-splitting Perfect Polynomials

p	Degree	Complete Factorization
2	5	$x(x-1)^2(x^2+x+1)$, $x^2(x-1)(x^2+x+1)$
	11	$x(x-1)^2(x^2+x+1)^2(x^4+x+1)$, $x^2(x-1)(x^2+x+1)^2(x^4+x+1)$
		$x^3(x-1)^4(x^4+x^3+1)$, $x^4(x-1)^3(x^4+x^3+x^2+x+1)$
	15	$x^3(x-1)^6(x^3+x+1)(x^3+x^2+1)$, $x^6(x-1)^3(x^3+x+1)(x^3+x^2+1)$
	16	$x^4(x-1)^4(x^4+x^3+1)(x^4+x^3+x^2+x+1)$
	20	$x^4(x-1)^6(x^3+x+1)(x^3+x^2+1)(x^4+x^3+x^2+x+1)$
		$x^6(x-1)^4(x^3+x+1)(x^3+x^2+1)(x^4+x^3+1)$
3	8	$x(x-1)^2(x-2)^3(x^2+2x+2)$, $x^2(x-1)^3(x-2)(x^2+x+2)$,
		$x^3(x-1)(x-2)^2(x^2+1)$
	15	$x^3(x-1)^3(x-2)^3(x^2+1)(x^2+x+2)(x^2+2x+2)$
	16	$x(x-1)^2(x-2)^4(x^2+1)(x^3+2x^2+x+1)(x^4+2x^3+x^2+x+2)$
		$x^2(x-1)^4(x-2)(x^2+2x+2)(x^3+2x^2+2x+2)(x^4+x^2+x+1)$
		$x^4(x-1)(x-2)^2(x^2+x+2)(x^3+2x^2+1)(x^4+x^3+x^2+x+1)$
3	23	$x^5(x-1)^5(x-2)^7(x^2+1)(x^2+x+2)(x^2+2x+2)$
		$x^5(x-1)^7(x-2)^5(x^2+1)(x^2+x+2)(x^2+2x+2)$
		$x^7(x-1)^5(x-2)^5(x^2+1)(x^2+x+2)(x^2+2x+2)$
	28	$x^5(x-1)^5(x-2)^6(x^6+x^5+2x^3+2x^2+1)(x^6+x^5+2x^3+2x^2+2)$
		$x^5(x-1)^6(x-2)^5(x^6+x^5+2x^4+2x^3+1)(x^6+x^5+2x^4+2x^3+2)$
		$x^6(x-1)^5(x-2)^5(x^6+x^5+x^4+x^3+x^2+x+1)(x^6+x^5+x^4+x^3+x^2+x+2)$
	39	$x^4(x-1)^4(x-2)^4(x^4+x^3+x^2+x+1)(x^4+2x^3+x^2+x+2)$
		$(x^4+x^2+x+1)(x^3+2x^2+1)(x^3+2x^2+x+1)(x^3+2x^2+2x+2)$
		$(x^2+1)(x^2+x+2)(x^2+2x+2)$

Continued: TABLE I.

p	Degree	Complete Factorization
	54	$x^6(x-1)^6(x-2)^6(x^6+x^5+x^4+x^3+x^2+x+1)$
		$(x^6+x^5+x^4+x^3+x^2+x+2)(x^6+x^5+2x^4+2x^3+1)$
		$(x^6+x^5+2x^4+2x^3+2)(x^6+x^5+2x^3+2x^2+1)$
		$(x^6+x^5+2x^3+2x^2+2)$
	75	$x^9(x-1)^9(x-2)^9(x^4+x^3+x^2+x+1)(x^4+2x^3+x^2+2x+1)$
		$(x^4+x^2+2x+1)(x^4+2x^3+x^2+x+2)(x^4+x^2+x+1)$
		$(x^4+x^3+x^2+2x+2)(x^3+2x^2+1)(x^3+x^2+2)(x^3+x^2+2x+1)$
		$(x^3+2x^2+x+1)(x^3+2x^2+2x+2)(x^3+x^2+x+2)(x^2+1)$
		$(x^2+x+2)(x^2+2x+2)$
5	22	$x^3(x-1)(x-2)^2(x-3)^2(x-4)^2(x^2+2)(x^2+3)(x^2+3x+3)$
		$(x^2+3x+4)(x^2+2x+3)(x^2+2x+4)$
		$x^2(x-1)^3(x-2)(x-3)^2(x-4)^2(x^2+x+1)(x^2+x+2)(x^2+2)$
		$(x^2+3)(x^2+3x+3)(x^2+3x+4)$
		$x^2(x-1)^2(x-2)^3(x-3)(x-4)^2(x^2+x+1)(x^2+x+2)$
		$(x^2+4x+1)(x^2+4x+2)(x^2+3x+3)(x^2+3x+4)$
		$x^2(x-1)^2(x-2)^2(x-3)^3(x-4)(x^2+x+1)(x^2+x+2)$
		$(x^2+4x+1)(x^2+4x+2)(x^2+2x+3)(x^2+2x+4)$
		$x(x-1)^2(x-2)^2(x-3)^2(x-4)^3(x^2+4x+1)(x^2+4x+2)$
		$(x^2+2x+3)(x^2+2x+4)(x^2+2)(x^2+3)$
	30	$x^2(x-1)^2(x-2)^2(x-3)^2(x-4)^2(x^2+x+1)(x^2+x+2)$
		$(x^2+3x+3)(x^2+3x+4)(x^2+2)(x^2+3)$
		$(x^2+2x+3)(x^2+2x+4)(x^2+4x+1)(x^2+4x+2)$
	36	$x(x-1)(x-2)^4(x-3)^4(x-4)^6(x^6+2x^5+x^4+x+2)$
		$(x^6+2x^5+x^4+x+3)(x^4+x^3+x^2+1)(x^2+4x+1)(x^2+4x+2)$
		$x(x-1)^4(x-2)^4(x-3)^6(x-4)(x^6+3x^5+x^4+4x^3+x^2+x+2)$
		$(x^6+3x^5+x^4+4x^3+x^2+x+3)(x^4+4x+4)(x^2+x+1)(x^2+x+2)$
		$x^4(x-1)^4(x-2)^6(x-3)(x-4)(x^6+4x^5+x^4+3x^3+4x^2+3)$
		$(x^6+4x^5+x^4+3x^3+4x^2+4)(x^4+4x^3+x^2+3x+4)$
		$(x^2+3x+3)(x^2+3x+4)$
		$x^4(x-1)^6(x-2)(x-3)(x-4)^4(x^6+x^4+2x^3+4x^2+2x+1)$
		$(x^6+x^4+2x^3+4x^2+2x+2)(x^4+3x^3+4x^2+x+3)(x^2+2)(x^2+3)$
5	36	$x^6(x-1)(x-2)(x-3)^4(x-4)^4(x^6+x^5+x^4+x^3+x^2+x+1)$
		$(x^6+x^5+x^4+x^3+x^2+x+2)(x^4+2x^3+4x^2+2x+2)$
		$(x^2+2x+3)(x^2+2x+4)$

Continued: TABLE I.

p	Degree	Complete Factorization
	85	$x^5(x-1)^5(x-2)^5(x-3)^5(x-4)^5(x^2+2)^2(x^2+x+1)^2(x^2+2x+3)^2$
		$(x^2+3x+3)^2(x^2+4x+1)^2(x^4+2)(x^4+3)$
		$(x^4+2x^3+4x^2+3x+3)(x^4+2x^3+4x^2+3x+4)$
		$(x^4+4x^3+x^2+4x+3)(x^4+4x^3+x^2+4x+4)$
		$(x^4+x^3+x^2+x+3)(x^4+x^3+x^2+x+4)$
		$(x^4+3x^3+4x^2+2x+3)(x^4+3x^3+4x^2+2x+4)$
	130	$x^6(x-1)^6(x-2)^6(x-3)^6(x-4)^6(x^6+x^5+x^4+x^3+x^2+x+1)$
		$(x^6+x^5+x^4+x^3+x^2+x+2)(x^6+x^4+2x^3+4x^2+2x+1)$
		$(x^6+x^4+2x^3+4x^2+2x+2)(x^6+4x^5+x^4+3x^3+4x^2+3)$
		$(x^6+4x^5+x^4+3x^3+4x^2+4)(x^6+3x^5+x^4+4x^3+x^2+x+2)$
		$(x^6+3x^5+x^4+4x^3+x^2+x+3)(x^6+2x^5+x^4+x+2)$
		$(x^6+2x^5+x^4+x+3)(x^4+2x^3+4x^2+2x+2)$
		$(x^4+3x^3+4x^2+x+3)$
		$(x^4+4x^3+x^2+3x+4)(x^4+4x+4)(x^4+x^3+x^2+1)$
		$(x^2+2x+3)(x^2+2x+4)(x^2+2)(x^2+3)(x^2+3x+3)$
		$(x^2+3x+4)(x^2+x+1)(x^2+x+2)(x^2+4x+1)(x^2+4x+2)$

REFERENCES

[1] E. F. CANADAY (1941) – *The sum of the divisors of a polynomial*, «Duke Math. J.», 7, 721–737.

[2] J. R. OCONNELL (1974) – *Perfect polynomials over* GF (p). Unpublished master's thesis, University of Texas at Arlington.