LIBERTAS MATHEMATICA, VOL. XVII (1997)

ITERATED SUMS OF POLYNOMIAL DIVISORS†

J. T. B. BEARD, JR. AND M. LEANNE LINK

In praise of His caregivers from the Book

and

In loving memory of

Jacob Thomas Barron & Mamie Green Beard

1908-1997 1912-1984

ABSTRACT

This study reinitiates the 1941 inquiry of E.F. Canaday, the first Ph.D. student of L. Carlitz, which was restricted to $F_2[x] = GF[2,x]$. Since 1974 one of us has focused on perfect, unitary perfect, bi-unitary perfect, and non-unitary perfect polynomials. Here, $F_q[x]$ is partitioned using maximal set-theoretic unions of directed (n,k)-bracelets $A_0 \to A_1 \to \ldots \to A_{k+n} = A_k$ where the monic polynomials $A_0, \ldots, A_{k+n-1}$ are distinct, $n \geq 1$, $k \geq 0$; with $A_i \to A_{i+1}$ denoting $\sigma(A_i) = A_{i+1}$ and $\sigma(A_i)$ the sum of the distinct monic divisors in $F_q[x]$ of the polynomial A_i. New constructions for perfect polynomials $(A \to A)$, disproof of the 1977 conjecture that x divides each perfect polynomial in $F_p[x]$, the existence of infinitely many pairs $A \neq B$ of amicable polynomials $(A \to B \to A)$, and digraph structures of computed maximal unions of non-disjoint bracelets are obtained.

1. INTRODUCTION. E.F. Canaday studied [10] the sum $\sigma(A)$ of the distinct divisors in $F_2[x]$ of polynomials $A = A(x) \in F_2[x]$. Later studies [1]-[9], [15], [17] of various polynomial analogs over F_q, $q = p^d$, $d \geq 1$, of number-theoretic phenomena have yielded numerous results and raised a variety of open questions. Here, Canaday's broad inquiry is reinitiated for $p > 2$. We use his notation and Harary's language [13].

As usual, F_p is represented by the ring of integers *modulo p*. Unless noted otherwise, our discussion is restricted to monic polynomials $A = A(x)$ in the integral domain $F_q[x]$, for which $\sigma(A)$ denotes the sum of the distinct monic polynomials $B \in F_q[x]$ which are divisors of A. We write $A \to C$ whenever $\sigma(A) = C$. Easily, the arithmetic function mapping $F_q[x]$ into the field $F_q(x)$ defined by $\sigma(cA) = c\sigma(A)$, $c \in F_q^*$, is multiplicative; i.e., $\sigma(AB) = \sigma(A)\sigma(B)$ whenever $(A,B) = 1$. Thus σ is completely determined by its values on the non-negative integral powers P^α of the *prime* (monic irreducible) polynomials: $\sigma(P^\alpha) = P^\alpha + P^{\alpha-1} + \cdots + 1 = \frac{P^{\alpha+1}-1}{P-1}$. Since A is the unique monic divisor of A having maximum degree, then σ is both monicicity and degree preserving on the $q^{\deg(A)}$ such monic polynomials A. Taking $\sigma^0(A) = A$, the sequence $\sigma|_A = \{\sigma^i(A)\}_{i\geq 0}$ is eventually perodic. In §2 we study a natural equivalence relation induced on $F_q[x]$ by these *orbits* $\sigma|_A$. Those basic examples and elementary results establish (§3) the infinitude of amicable polynomials $A \neq B$, $A \to B \to A$ over $F_q[x]$, $q = p^d$, for infinitely many primes p and infinitely many integers $d \geq 1$. In §4 we exhibit perfect polynomials over F_{11}, F_{17} which are not divisible by x, refuting a conjecture [2] of the first author.

2. RING-EQUIVALENCE ON $F_q[x]$. Clearly, $F_q[x]$ is partitioned by the scalar multiples over F_q of the monic polynomials $F_q[x]_M$, and the latter are partitioned according to their degrees e, say $F_q[x]_M = \cup_{e\geq 0} F_{q,e}[x]$. Refine these partitions further:

Definition 1. The sequence of monic polynomials $\mathcal{B}(n,k,A)$ given by $A = A_0 \to A_1 \to \ldots \to A_{k+n} = A_k$, where $A_0, A_1, \ldots, A_{k+n-1} \in F_q[x]$ are distinct, is called the *cyclic (n,k)-bracelet generated by A* over F_q. The subsequence $\mathcal{R}(A) = \mathcal{R}(n,A) = \{A_k, \ldots, A_{k+n-1}\}$, is called the *$n$-ring determined by A* if $k > 0$; otherwise, the *n-ring generated* by A. A *bracelet* in $F_q[x]$ is an arbitrary nonempty set-theoretic union of non-disjoint cyclic bracelets generated by monic polynomials $A \in F_q[x]$.■

Definition 2. Polynomials $A, B \in F_q[x]$ are called *ring-equivalent* provided $\mathcal{R}(A) = \mathcal{R}(B)$ set-theoretically, in which case we write $A\mathcal{R}B$.■

Evidently, $\mathcal{R}$-equivalence is an equivalence relation on $F_q[x]_M$ and on each $F_{q,e}[x], e \geq 1$. The $\mathcal{R}$-equivalence classes are the maximal bracelets given by the set-theoretic unions of the non-disjoint iterates of σ "acting" on $F_{q,e}[x]$. I.e., $F_{q,e}[x]$ is partioned by the maximal unions $\overline{\mathcal{B}}$ of non-disjoint orbits $\sigma|_A$, $A \in F_{q,e}[x]$, determined by the finite cyclic semigroup $< \sigma >$. Graph-theoretically: The (obvious) *σ-digraph* $F_q^\sigma[x]$ has infinitely many components, each of which is finite, simple (no multiple edges), and unicyclic with loops, the deletion of whose cycle-edges results in a forest of in-trees having the cycle-vertices as sinks. The structure of finite cyclic semigroups (such as $< \sigma >$) has been understood since Frobenius [11; p. 20], but it seems the orbits under their "action" on sets have been studied only probabilisticly [14], and even Carlitz' classroom lecture notes "The Arithmetic of Polynomials" do not contain applicable arithmetic-function theory. We proceed accordingly.

Theorem 1. *If $A \in F_{q,1}[x], q = p^d, d \geq 1$, then the cyclic bracelet $\mathcal{B}(A)$ is a p-ring.*

Proof. Since A is prime, $\mathcal{B}(A) = A + F_p$ (the additive left coset of F_p in $F_q[x]$).■

An earlier argument [4; Theorem 7] establishes:

Theorem 2. *Let $A(x), B(x) \in F_q[x]$ be monic polynomials, $q = p^d, d \geq 1$. Then $\sigma(A(x)) = \sigma(B(x))$ if and only if $\sigma(A(x+c)) = \sigma(B(x+c))$ for all $c \in F_q$.*■

Note: Distinct translates of polynomials are not necessarily distinct: consider $P(x) = x^3 + 2x + 1 \in F_3[x]$.

If $\sigma(A)$ is a prime then A is a prime-power; this is "best possible": $\sigma((x+i)^2) \in F_5(x)$ is prime, $0 \leq i \leq 4$. Examination of $F_{3,3}[x]$ establishes: If $\sigma(A)$ is a prime-power then "all possibilities" for A are realized. One may apply Theorem 2 to the following "root-results" and translate them across $F_p[x]$ or lift them to $F_q[x]$.

Theorem 3. *Let $x \in F_p[x]$ and $\alpha \geq 1$. Then $x|\sigma[(x+1)^\alpha]$ if and only if $\alpha \equiv -1 (mod\ p)$.*

Proof. Clearly, $\sigma[(x+1)^\alpha] = \sum_{i=0}^{\alpha}(x+1)^i$ has value 0 at $x = 0$ if and only if $\alpha + 1 \equiv 0 (mod\ p)$.■

Corollary 4. *Let $P \in F_p[x]$ be prime, $P \not\equiv 1$ but $P(j) = 1$ for some $j \in F_p$. Then $(x-j)|\sigma(P^\alpha)$ if and only if $\alpha \equiv -1 (mod\ p)$.*■

Theorem 5. *Let $P \in F_p[x]$ be prime with $1 < P(j) < p$ for some $j \in F_p$. Then $(x-j)|\sigma(P^\alpha)$ whenever $\alpha \equiv -1(mod\ (p-1))$.*

Proof. Let $a, j \in F_p$ satisfy $1 < P(j) = a < p$, and consider

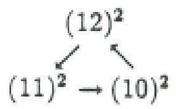
$$(*) \qquad (\sigma[P^\alpha(x)])|_{x=j} = \textstyle\sum_{i=0}^{\alpha} a^i.$$

Since $a \in F_p^*$ has multiplicative order dividing $p-1$, and $\sum_{i=0}^{p-2} a^i \equiv 0(mod\ p)$ from Euler's Theorem, then the number $\alpha + 1 = m(p-1)$ of terms in $(*)$ is sufficient for the claim.■

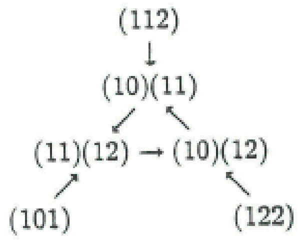
In the course of exhibiting the σ-digraphs which complete this section, we have benefited from discussions with Ann D. Dorris. (Using his personalized/programmable GALOIS II) Rex Matthews has *amicably* provided us with $\sigma(A)$ for $A \in F_{5,4}[x]$ and calculations to double-check our examples. We especially appreciate the dedication of Vickie Mayberry, who has produced our digraphs (using Windows' Paintbrush and TEX). The 600-vertex $F_{5,4}^{\sigma}[x]$ remains under construction (using Maple V). For conciseness represent $A(x) = x^n + a_1x^{n-1} + \cdots + a_n$ by $(1a_1 \cdots a_n)$, and its digraph vertex by the base 10 integer k determined by the base q integer $a_1a_2\ldots a_n$. I.e., $k = A(q) - q^n$ for the *rational integral* polynomial $A(x)$. The distribution of the prime polynomials is exhibited appropriately.

Example 1. $F_{3,2}[x] = \overline{B}_1 \cup \overline{B}_2$ as follows:

$\overline{B}_1$:

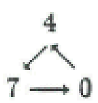


$\overline{B}_2$:

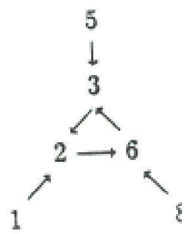


$F_{3,2}^{\sigma}[x]$ is given by:

$\overline{B}_1$:



$\overline{B}_2$:



Example 2. $F_{3,3}[x] = \overline{B}_1 \cup \overline{B}_2 \cup \overline{B}_3 \cup \overline{B}_4$ where

$\overline{B}_1$:

$$\left.\begin{array}{ccc} (1201) & \longrightarrow & (11)(112) \\ (1211) & \longrightarrow & (12)(101) \\ (1222) & \longrightarrow & (10)(122) \\ (1021) & \longrightarrow & (1022) \end{array}\right\} \rightarrow (10)(11)(12) \circlearrowleft$$

$\overline{B}_2$:

$$\begin{array}{ccccc} & (1112) & & (10)^2(12) & \\ & \searrow & \swarrow & \nwarrow & \\ & & (10)(112) & & (12)(122) \\ & \nearrow & \searrow & \nearrow & \\ (11)(122) & & & (11)^3 & \end{array}$$

$\overline{B}_3$:

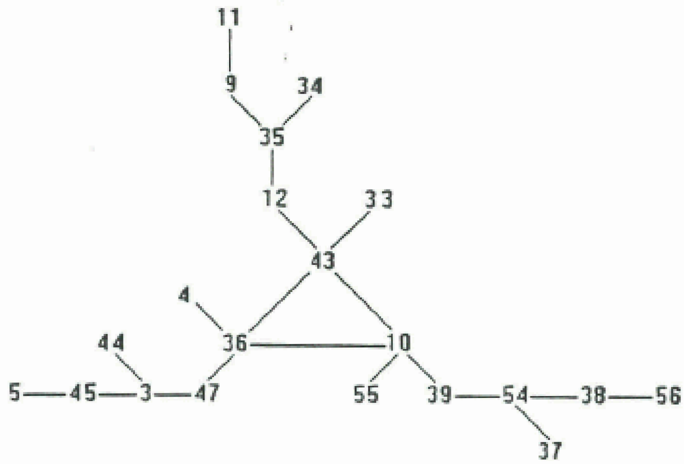
$$\begin{array}{ccccc} & (1102) & & (10)(11)^2 & \\ & \searrow & \swarrow & \nwarrow & \\ & & (10)^2(11) & & (11)^2(12) \\ & \nearrow & \searrow & \nearrow & \\ (12)(112) & & & (12)^3 & \end{array}$$

$\overline{B}_4$:

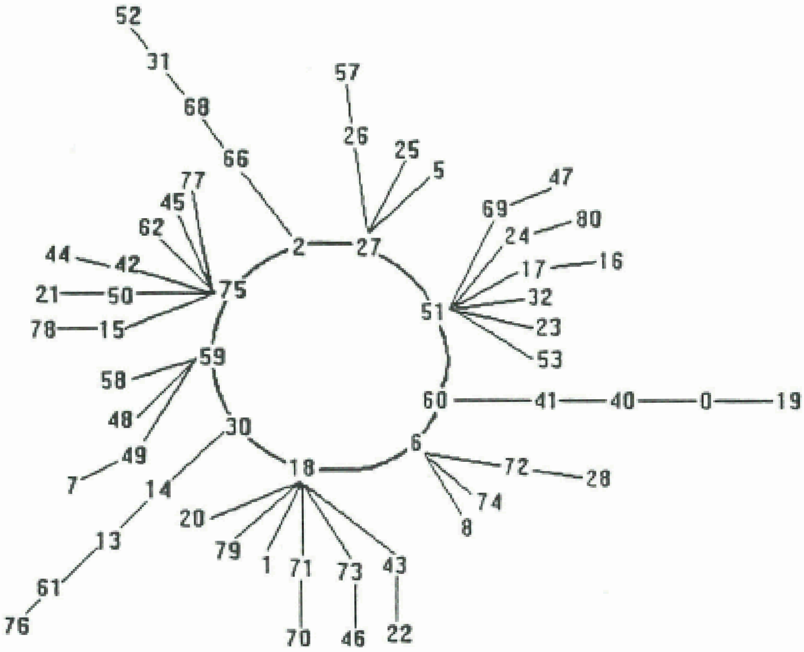
$$\begin{array}{ccccc} & (1121) & & (10)(11)^2 & \\ & \searrow & \swarrow & \nwarrow & \\ & & (10)(11)^2 & & (11)^2(12) \\ & \nearrow & \searrow & \nearrow & \\ (10)(101) & & & (10)^3 & \end{array}$$

Example 3. $F^{\sigma}_{3,4}[x] = \overline{B}_1 \cup \overline{B}_2$ where

$\overline{B}_1$ 21 polynomials; 6/18 primes. :



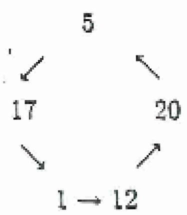
$\overline{B}_2$ 60 polynomials; 12/18 primes. :



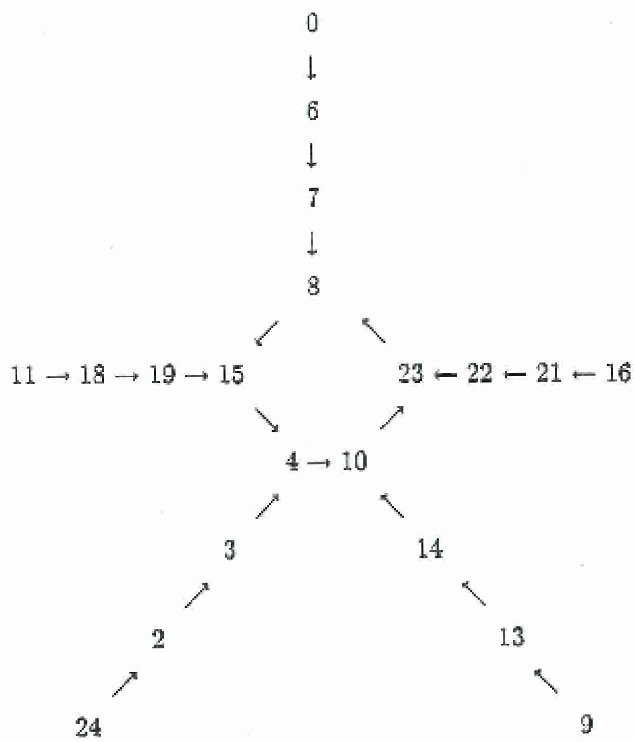
■

Example 4. $F^{\sigma}_{5,2}[x] = \overline{\mathcal{B}}_1 \cup \overline{\mathcal{B}}_2$ where

$\overline{\mathcal{B}}_1$ | 5 polynomials; 0/10 primes. | :

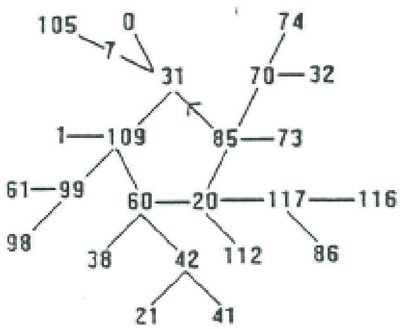


$\overline{\mathcal{B}}_2$ | 20 polynomials; 10/10 primes. | :

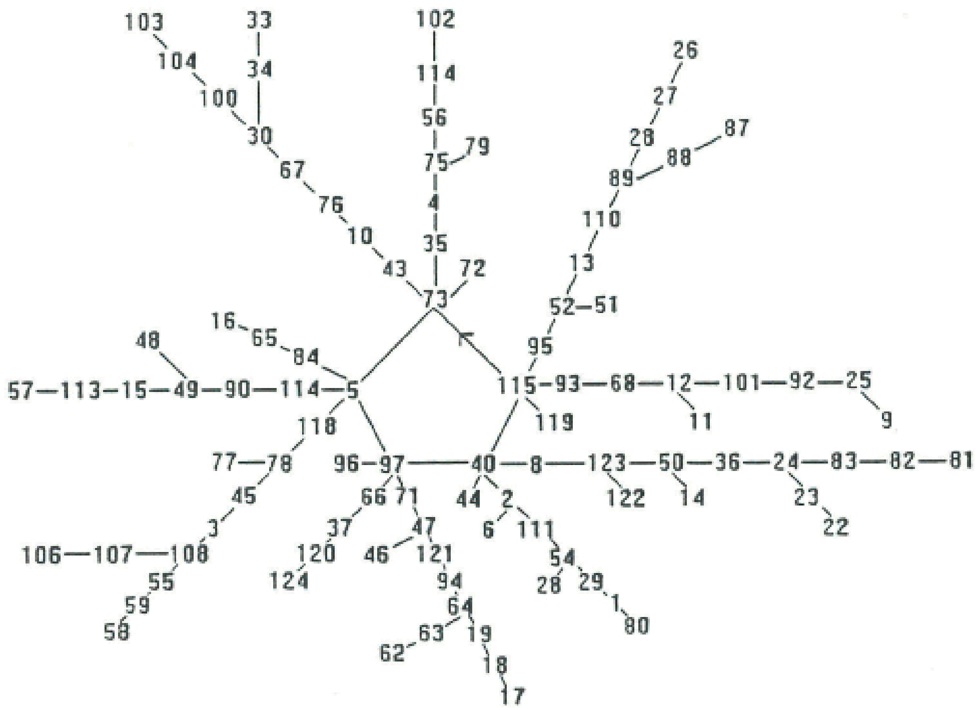


Example 5. $F^{\sigma}_{5,3}[x] = \overline{B}_1 \cup \overline{B}_2$ where

$\overline{B}_1$ [24 polynomials; 4/40 primes.] :



$\overline{B}_2$ [101 polynomials; 36/40 primes.] :



■

3. CYCLIC (p,k)-BRACELETS AND p-RINGS. We now determine the cyclic bracelets generated by specific polynomials of "low" degrees, but have not improved the trivial bounds on cyclic (n,k)-bracelets generated by polynomials of degree $e > 2$ over F_q: $n \geq 1$, $k \geq 0$, $n + k \leq q^e$. First, a general construction technique.

Theorem 6. *The polynomial $A(x) \in F_q[x]$ generates an (n,k)-bracelet if and only if $B_c(x) = A(x+c)$ generates an (n,k)-bracelet for each $c \in F_q$.*

Proof. By finite induction using Theorem 2.■

Our next results extend Theorem 1.

Theorem 7. *Let $c \in F_q$, $q = p^d, d \geq 1$, and $\emptyset \subset \Lambda \subset F_q$. Then $A = \Pi_{i\in\Lambda}(x + c - i)$ generates a p-ring.*

Proof. From Theorem 6, set $c = 0$ w.l.o.g. By Theorem 1, each polynomial $(x - i)$ generates a p-ring. Since $(x - i, x - j) = 1$ for $i \neq j$, and σ is multiplicative, then $A \to \Pi_{i\in\Lambda}\sigma(x-i) = \Pi_{i\in\Lambda}(x-i+1)$. By finite induction, $\sigma^p[\Pi_{i\in\Lambda}(x-i)] = \Pi_{i\in\Lambda}(x-i) = A$. Since $\Lambda \neq F_q$, p is the smallest positive l satisfying $\sigma^l(A) = A$.■

Corollary 8. *Let $A = \Pi_{\alpha\in\Lambda}(x - \alpha) \in F_q[x], q = p^d, d \geq 1$, and let $\Lambda \subset F_q$ have a non-empty proper intersection with at least one of the additive cosets in F_q/F_p. Then A generates a p-ring.*■

Theorem 9. *If $c \in F_q$ and $n \geq 0$, then $(x+c)^{p^n-1}$ generates a p-ring.*

Proof. Set $c = 0$ and note that $x^{p^n-1} \to (x-1)^{p^n-1}$, so $\sigma^p(x^{p^n-1}) = x^{p^n-1}$ and p is the smallest such power of σ.■

Corollary 10. *Let $A = \Pi_{\alpha\in\Lambda}(x-\alpha)^{p^{n(\alpha)}-1} \in F_q[x]$, $q = p^d, d \geq 1$, $n(\alpha) > 0$. If $\Lambda \subset F_q$ has a non-empty proper intersection with at least one additive coset in F_q/F_p, then A generates a p-ring over F_q.*■

Corollary 11. *Whenever $c \in F_q$, $q = p^d, d \geq 1$ and $n(0), \ldots, n(p-1) > 0$ are not all equal, then $A = \Pi_{i=0}^{p-1}(x+c-i)^{p^{n(i)}-1}$ generates a p-ring.*

Proof. Note that $(x-i)^{p^{n(i)}-1} \to (x-i-1)^{p^{n(i)}-1} = [x-(i+1)]^{p^{n(i)}-1}$.■

Hereafter, we restrict our attention to the case $q = p > 2$, and appeal to Legendre symbols $(\frac{a}{p})$ and the distribution of quadratic residues.

Theorem 12. *If $p \equiv 1, 7 (mod\ 12)$, then $x^2 \in F_p[x]$ generates a $(p,1)$-bracelet.*

Proof. For $p \equiv 1, 7(mod\ 12)$, the discriminant of $\sigma(x^2) = x^2 + x + 1$ is $d = -3$. Since $\left(\frac{-3}{p}\right) = 1$ then $x^2+x+1 = (x+j)(x+i)$ for distinct $i, j \in F_p$. By Theorem 7, $(x+j)(x+i)$ generates a p-ring as $p > 3$. Thus x^2 generates a $(p,1)$-bracelet.■

Theorem 13. *If $p \equiv 11, 23, 29, 53, 65, 71 (mod\ 84)$, then $x^2 \in F_p[x]$ generates a $(p,2)$-bracelet.*

Proof. Since $p \equiv 11, 23, 29, 53, 65, 71(mod\ 84)$, then $p \equiv 5, 11(mod\ 12)$, $\sigma(x^2)$ has discriminant $d = -3$, and $\left(\frac{-3}{p}\right) = -1$. Thus $\sigma(x^2)$ is a prime. The discriminant of $\sigma^2(x^2) = x^2 + x + 2$ is $d = -7$ and $p \equiv 1, 9, 11, 15, 23, 25(mod\ 28)$, thus $\left(\frac{-7}{p}\right) = 1$. Hence $\sigma^2(x^2) = (x+i)(x+j)$ for distinct $i, j \in F_p$. By Theorem 7 $(x+j)(x+i)$ generates a p-ring, hence x^2 generates a $(p,2)$-bracelet.■

Theorem 14. *If $p \equiv 1(mod\ 4)$, then $x^3 \in F_p[x]$ generates a $(p,1)$-bracelet.*■

Theorem 15. *If $p \equiv 3(mod\ 8)$ and $p \geq 11$, then $x^3 \in F_p[x]$ generates a $(p,2)$-bracelet.*

Proof. Note that $\sigma(x^3) = x^3 + x^2 + x + 1 = (x+1)(x^2+1)$ and the discriminant of x^2+1 is $d = -4$. Since $p \equiv 3(mod\ 4)$ then $\left(\frac{-1}{p}\right) = -1$, hence x^2+1 is prime. Thus $\sigma^2(x^3) = (x+2)(x^2+2)$. The discriminant of x^2+2 is $d = -8$, and $\left(\frac{-2}{p}\right) = 1$. Hence $\sigma^2(x^3) = (x+2)(x+\sqrt{-2})(x-\sqrt{-2})$. Since its roots are distinct and $p > 3$, then $\sigma^2(x^3)$ generates a p-ring.■

Theorem 16. *If $p > 2$ and $x^2 \in F_p[x]$ generates an (n,k)-bracelet, then $n = p$ and $k \leq \frac{p+1}{2}$.*

Proof. The n-ring of the bracelet is generated by the quadratic $x^2 + x + c$ which "first factors" for $c \in F_p$ under the "ordering" $1 < 2 < \ldots < p$. If $p > 2$ then $n = p$ by Theorem 7, and $x^2 + x + c$ factors if and only if $\left(\frac{1-4c}{p}\right) \neq -1$. Since there are $(p-1)/2$ nonzero quadratic residues in F_p, then there are at most $(p-1)/2$ "consecutive" primes of the form $x^2 + x + c$. Hence $\sigma^{(p+1)/2}(x^2)$ is in the p-ring determined by x^2.■

4. PERFECT POLYNOMIALS NOT DIVISIBLE BY x. Canaday [10] did not find any perfect polynomials over F_2 not divisible by x, and found it plausible that none exist. The exceptional condition proved by him was generalized [2]:

Fact 1. *Every perfect polynomial over $GF(2)$ is either divisible by $x(x-1)$ or else is a perfect square.*■

Fact 2. *If the polynomial $A = \Pi_{i=1}^{k} P_i^{n(i)}$ is perfect over F_p for $n(i) > 0$ and distinct primes P_i having constant terms c_i, then $x|A$ unless all of the following are satisfied:*

(*i*) $(\Pi_{j=0}^{p-1}(x-j), A) = 1$,

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

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

(*iv*) $n(i) \not\equiv -2(mod\ p-2)$ *whenever* $1 < c_i < p-1$. ■

The conjecture [2] "If A is perfect over F_p then $x|A$" of Beard is false as shown by Link [15]. Her three counter-examples follow in reverse historical order of their constructions (with $(1, a_1, \cdots, a_n) = x^n + a_1 x^{n-1} + \cdots + a_n$).

Example 6. For B=(1,0,1)(1,3,6)(1,8,5)(1,1,4)(1,4,5)(1,7,5)(1,2,2) (1,6,10)(1,9,2)·(1,5,10)(1,10,4)$\in F_{11}[x]$, $A = B^2$ is perfect over F_{11}.■

She also found a perfect polynomial not divisible by x and not a square, but first:

Definition 3. The monic polynomials $A, B \in F_q[x]$ are k-*amicable* over F_q provided $\sigma^k(A) = B$ and $\sigma^k(B) = A$. Whenever A, B are k-amicable and $A \neq B$, then we call A, B a k-*amicable pair* and write $(A,B)_{k-am}$. For $k = 1$ we merely say *amicable*.■

Example 7. Let $A = B^2C \in F_{17}[x]$ where B=(1,4,1)(1,13,1)(1,6,6)(1,15,15)(1,8,13)·(1,14)(1,2,15)(1,10,5)(1,14,12)(1,12,16)(1,16,10)(1,1,10)(1,3,12)(1,5,16)(1,7,5)(1,9,13)·(1,11,16) and C=(1,8,2,12,3)(1,9,2,5,3)(1,12,15,10,9)(1,13,1,6,3)(1,16,6,12,13)(1,12,7)·(1,4,1,11,3)(1,3,9,8,14)(1,11,10,4)(1,7,7,5,1)(1,15,5,13,9)(1,2,5,4,9)(1,6,7,4)·(1,10,7,12,1)(1,14,9,9,14)(1,1,6,5,14)(1,5,15,7,10). $B^2 \to C \to B^2$ and $(B^2, C) = 1$, so A is perfect.■

Finally, Link's Monster (of degree 476):

Example 8. Let $A = B^2C \in F_{17}[x]$ where B=(1,1,1)(1,3,3)(1,16,1)(1,7,13)(1,9,4)·(1,11,14)(1,13,9)(1,15,6)(1,0,5)(1,2,6)(1,4,9)(1,6,14)(1,8,4)(1,10,13)(1,12,7)(1,14,3)(1,5,7)·(1,15,13)(1,4,16)(1,6,4)(1,12)(1,13,16)(1,2,13)(1,10,3)(1,12,14)(1,8,11)(1,14,10)(1,16,8)·(1,1,8)(1,3,10)(1,5,14)(1,7,3)(1,9,11)(1,11,4)(1,7,11)(1,6,12)(1,13,7)(1,12,5)(1,15,4)·(1,14,1)(1,9,2)(1,8,2)(1,5,5)(1,4,7)(1,11,12)(1,10,11)(1,1,16)(1,2,4)(1,3,1)(1,16,16)(1,0,3)·(1,10,1)(1,4,14)(1,9,9)(1,3,8)(1,16,6)(1,15,11)(1,12,12)(1,1,6)(1,11,2)(1,10)(1,6,2)(1,5,12)·(1,8,9)(1,2,11)(1,7,1)(1,13,14)(1,14,8)(1,4,15)(1,16,7)(1,10,2)(1,15,12)(1,3,9)(1,14,9)·(1,9,10)(1,5,13)(1,6,3)(1,1,7)(1,7,2)(1,12,13)(1,11)(1,11,3)(1,2,12)(1,13,15)(1,8,10) and C=(1,2,4,3,3)(1,6,16,4,13)(1,15,4,14,3)(1,14,8,2,13)(1,1,5,13,4)(1,5,14,13,7)(1,9,1,9,6)·(1,13,8,9)(1,11,14)(1,4,9,9)(1,8,1,8,6)(1,12,14,4,7)(1,16,5,4,4)(1,3,8,15,13)(1,7,6,10,6)·(1,11,16,13,13)(1,10,6,7,6)(1,8,13,5,13)(1,15,16,2,6)(1,3,3,16,7)(1,13,12,1,4)(1,6,11,6,6)·(1,11,11,11,6)(1,1,2,9)(1,10,1,16,13)(1,12,9,8,13)(1,2,16,15,6)(1,14,3,1,7)(1,7,1,1,13)·(1,6,14)(1,5,9,9,13)(1,4,12,16,4)(1,9,13,12,3)(1,16,15,9). Then $\Pi_{i=0}^{16}((x+i)^2+5)^2 \to \Pi_{i=0}^{16}((x+i)^4+11(x+i)^2+14) \to \Pi_{i=0}^{16}((x+i)^2+12)^2 \to \Pi_{i=0}^{16}((x+i)^2+3)^2 \to \Pi_{i=0}^{16}((x+i)^2+10)^2 \to \Pi_{i=0}^{16}((x+i)^2+11)^2 \to \Pi_{i=0}^{16}((x+i)^4+6(x+i)^2+14) \to \Pi_{i=0}^{16}((x+i)^2+5)^2$. ■

Example 7 shows a new technique for constructing perfect polynomials:

Theorem 17. *Let $A, B \in F_q[x]$ and $(A,B) = 1$. If $(A,B)_{am}$ then AB is perfect.* ■

Corollary. *If $A \in F_q[x]$ generates an n-ring of pairwise relatively prime A_i, then $\Pi_{i=0}^{n-1} A_i$ is perfect.* ■

The converse of Theorem 17 is false:

Example 9. Let $A = B^2C(x^{17}-x) \in F_{17}[x]$ with B, C from Example 8. Since B^2C and $x^{17} - x = \Pi_{i=0}^{16}(x-i)$ are perfect, and $(B^2C, x^{17}-x) = 1$, then A is perfect. No factorization $A = DE$ with $(D,E) = 1$ yields $(D,E)_{am}$. ■

5. Amicable Pairs and Other even-Rings. The amicable pairs $(A, \sigma(A))_{am}$ over F_p given in Table I for $3 \le p \le 17$ were obtained by hand using [9] or on a PC using the GALOIS package of Lidl, Matthews, and Wells. For brevity, the five amicable pairs and infinite class over $GF(2)$ which Canady discovered [10] are not included, and those constructible from our theoretical results are omitted. For conciseness, let $x_i = x + i$.

TABLE 1

p	$(A,B)_{am}$
3	$A = (x^3-x)^3, B = (x^3-x)\Pi_{i=0}^{2}(x_i^2+1)$
3	$A = (x^3-x)^4\Pi_{i=0}^{2}(x_i^3+2x_i^2+1), B = (x^3-x)\Pi_{i=0}^{2}(x_i^2+1)\Pi_{i=0}^{2}\sum_{j=0}^{4} x_i^j$
3	$A = (x^3-x)^7\Pi_{i=0}^{2}(x_i^4+2x_i^2+2), B = (x^3-x)^5\Pi_{i=0}^{2}(x_i^2+1)^3$ $\cdot\Pi_{i=0}^{2}(x_i^4+2x_i^3+x_i^2+2x_i+1)$
3	$A = (x^3-x)^9\Pi_{i=0}^{2}(x_i^3+2x_i^2+1)\Pi_{i=0}^{2}(x_i^3+x_i^2+2), B = (x^3-x)^5$ $\cdot\Pi_{i=0}^{2}(x_i^2+1)\Pi_{i=0}^{2}\sum_{j=0}^{4} x_i^j\Pi_{i=0}^{2}(x_i^4+2x_i^3+x_i^2+2x_i+1)$

p	$(A,B)_{am}$
3	$A=(x^3-x)^{10}\Pi_{i=0}^{2}(x_i^2+1)(x_i^3+x_i^2+2), B=(x^3-x)^5$ $\cdot\Pi_{i=0}^{2}(x_i^5+x_i^4+2x_i+1)\Pi_{i=0}^{2}(x_i^5+2x_i^4+2x_i^3+2x_i+1)$
3	$A=(x^3-x)^{19}\Pi_{i=0}^{2}(x_i^3+x_i^2+2)(x_i^3+2x_i^2+1), B=(x^3-x)^5$ $\cdot\Pi_{i=0}^{2}(x_i^2+1)^2(x_i^4+x_i^2+2x_i+1)\Pi_{i=0}^{2}(x_i^4+x_i^2+x_i+1)(x_i^4+x_i+2)$ $\cdot\Pi_{i=0}^{2}(x_i^4+2x_i+2)$
3	$A=(x^3-x)^{27}\Pi_{i=0}^{2}(x_i^2+1)^2\Pi_{i=0}^{2}\sum_{j=1}^{6}(x_i^j+2)\Pi_{i=o}^{2}(x_i^6+2x_i^5+x_i^4+2x_i^3+2x_i+1)$ $B=(x^3-x)^{17}\Pi_{i=0}^{2}(x_i^2+1)\Pi_{i=0}^{2}\sum_{j=0}^{6}x_i^j\Pi_{i=0}^{2}(x_i^6+x_i^5+x_i^3+1)$ $\cdot\Pi_{i=0}^{2}(x_i^6+2x_i^5+2x_i^3+2x_i+1)\Pi_{i=0}^{2}(x_i^6+2x_i^5+x_i^4+2x_i^3+x_i^2+2x_i+1)$
5	$A=(x^5-x)^5\Pi_{i=0}^{4}(x_i^4+1), B=(x^5-x)\Pi_{i=0}^{4}(x_i^2+2)^2(x_i+3)$
5	$A=(x^5-x)^{13}\Pi_{i=0}^{4}(x_i^2+2)^2(x_i^4+3)\Pi_{i=0}^{4}\sum_{j=1}^{6}(x_i^j+2)\Pi_{i=0}^{4}(x_i^6+3x_i^5+x_i^4+4x_i+3),$ $B=(x^5-x)^9\Pi_{i=0}^{4}(x_i^4+2)(x_i^4+x_i+4)\Pi_{i=0}^{4}(x_i^4+4x_1+4)\Pi_{i=0}^{4}\sum_{j=0}^{6}(x_i^j)$ $\cdot\Pi_{i=0}^{4}(x_i^6+3x_i^5+x_i^4+4x_i+2)$
5	$A=(x^5-x)^{15}\Pi_{i=0}^{4}(x_i^2+3)^2(x_i^4+3), B=(x^5-x)^9\Pi_{i=0}^{4}(x_i^2+2)(x_i^2+3)(x_i^4+2)(x_i^4+3)$
7	$A=(x^7-x)^2\Pi_{i=0}^{6}\sum_{j=1}^{4}(x_i^j+2), B=(x^7-x)^2\Pi_{i=0}^{6}(x_i^2+4)\Pi_{i=0}^{6}\sum_{j=0}^{4}x_i^j$
11	$A=(x^{11}-x)^6, B=\Pi_{i=0}^{10}(x_i^3+7x_i^2+6x_i+10)\Pi_{i=0}^{10}(x_i^3+5x_i^2+4x_i+10)$
13	$A=(x^{13}-x)^4\Pi_{i=0}^{12}(x_i^2+11)\Pi_{i=0}^{12}\sum_{j=1}^{4}x_i^j+2), B=(x^{13}-x)^3$ $\cdot\Pi_{i=0}^{12}(x_i^3+7x_i+7x_i+7)\Pi_{i=0}^{12}\sum_{j=0}^{4}x_i^j$
13	$A=(x^{13}-x)^6\Pi_{i=0}^{12}(x_i^2+6)(x_i^2+8), B=(x^{13}-x)^2$ $\cdot\Pi_{i=0}^{12}(x_i^2+2)(x_i^2+5)(x_i^2+7)(x_i^2+11)$
13	$A=(x^{13}-x)^7\Pi_{i=0}^{12}(x_i^2+6)(x_i^2+8), B=(x^{13}-x)^5\Pi_{i=0}^{12}(x_i^2+5)(x_i^2+7)(x_i^2+8)$
13	$A=(x^{13}-x)^8\Pi_{i=0}^{12}(x_i^3+11), B=(x^{13}-x)^5\Pi_{i=0}^{12}(x_i^3+4)(x_i^3+10)$
17	$A=\Pi_{i=0}^{16}(x_i^2+14)^2, B=\Pi_{i=0}^{16}(x_i^4+12x_i^2+7)$ ■

To construct amicable pairs, recall Example 9, Theorem 17, and from [2],[8]:

Fact 3. *The polynomial* $A=\Pi_{i=0}^{p-1}(x-i)^{n(i)}\in F_p[x]$ *is perfect if and only if* $n(0)=\ldots=n(p-1)=Np^n-1$ *where* $N|(p-1)$ *and* $n\geq 0$.■

Theorem 18. *Let* $A,B,C\in F_q[x]$ *be pairwise relatively prime. Then* A *is perfect and* $(B,C)_{am}$ *if and only if* $(AB,AC)_{am}$.

Proof. The necessity of $(AB,AC)_{am}$ is evident. Conversely, we have $\sigma(A)\sigma(B)=AC$ and $\sigma(A)\sigma(C)=AB$, from which $\sigma(A)\sigma(B)\sigma(C)=AC\sigma(C)=AB\sigma(B)$. So $C\sigma(C)=B\sigma(B)$, $C|\sigma(B)$, and $B|\sigma(C)$. Since $(AB,AC)_{am}$ and σ is degree-preserving, then $\deg B=\deg C$. Since $\sigma(B)$ is the unique monic divisor of itself having maximum degree then $C=\sigma(B)$. By symmetry, $B=\sigma(C)$. Since $B\neq C$ then $(B,C)_{am}$. Finally, $\sigma(A)\sigma(B)=AC=A\sigma(B)$ so $\sigma(A)=A$.■

Example 10. There exist infinitely many amicable pairs of polynomials over F_q for $q=17^d$, d odd, by Fact 3 and Theorem 18: B^2,C of Example 8 are relatively prime to $x^{17}-x$; $n\geq 0$ is arbitrary in Fact 3; and the prime factors of B^2,C remain prime over F_q [12].■

From Dirichlet's theorem on the infinitude of primes in an arithmetic progression, the next three results each establish that $(A,\sigma(A))_{am}$ exist for infinitely many odd primes p.

Lemma 1. *If $p \geq 3$ and $c, i, j \in F_p$ with $i \neq j$, the translates $(x+i)^2+(x+i)+c$ and $(x+j)^2+(x+j)+c$ are distinct.*■

Theorem 19. *The polynomials $A=(x^p-x)^2$, $\sigma(A) \in F_p[x]$ are amicable if and only if $p \equiv 11, 23, 29, 53, 65, 71 (mod\ 84)$.*

Proof. If $p=2$, then $A=(x^2-x)^2 \rightarrow x^4+x+1 \rightarrow x(x+1)^3$ so that A and $\sigma(A)$ are not amicable. If $p=3$, then $(x^3-x)^2 \leftrightarrow (x^3-x)^2$ and $A=(x^3-x)^2$ is perfect. Thus let $p \geq 5$ hereafter. Note that the discriminant of $\sigma(x^2)=x^2+x+1$ is $d=-3$ and $(\frac{3}{p}) \neq 0$. If $(\frac{-3}{p})=1$, then $\sigma(x^2)=(x+i)(x+j)$ for distinct $i, j \in F_p$. Thus from Lemma 1, $\sigma((x^p-x)^2)=(x^p-x)^2$ so A is perfect, hence A and $\sigma(A)$ are not an amicable pair over F_p. Hence assume $(\frac{-3}{p})=-1$, which occurs if and only if $p \equiv 5, 11 (mod\ 12)$. Then x^2+x+1 is prime over F_p. Thus $(x^p-x)^2 \rightarrow \Pi_{i=0}^{p-1}((x+i)^2+(x+i)+1)$ by Theorem 2 and is in canonical form by Lemma 1. Assume A and $\sigma(A)$ are amicable over F_p. Then $\sigma^2(x^2)|(x^p-x)^2$, so $\sigma^2(x^2)=\sigma(x^2+x+1)=x^2+x+2$ factors. Since the discriminant of x^2+x+2 is $d=-7$, then x^2+x+2 factors if and only if $(\frac{-7}{p})=1$ or $p=7$. Since $p \equiv 5, 11 (mod\ 12)$, then $p \neq 7$. Hence $(\frac{-7}{p})=1$, which occurs if and only if $p \equiv 1, 3, 9, 19, 25, 27 (mod\ 28)$. Solving the system of congruences

$$\begin{cases} p \equiv 5, 11 (mod\ 12) \\ p \equiv 1, 3, 9, 19, 25, 27 (mod\ 28) \end{cases} \quad \text{yields } p \equiv 11, 23, 29, 53, 65, 71 (mod\ 84).$$

Conversely, assume $p \equiv 11, 23, 29, 53, 65, 71 (mod\ 84)$. Then $p \equiv 5, 11 (mod\ 12), (\frac{-3}{p})=-1$, and x^2+x+1 is prime, so that $(x^p-x)^2 \rightarrow \Pi_{i=0}^{p-1}((x+i)^2+(x+i)+1)$. By Theorem 2 and Lemma 1, $\sigma(\Pi_{i=0}^{p-1}((x+i)^2+(x+i)+1))=\Pi_{i=0}^{p-1}(\sigma((x+i)^2+(x+i)+1))$. Since the discriminant of x^2+x+1 is $d=-7$ and $p \equiv 1, 3, 9, 19, 25, 27 (mod\ 28)$, then $(\frac{-7}{p})=1$, so that $\sigma(x^2+x+1)=(x+j)(x+l)$ for distinct $l, j \in F_p$. By Theorem 2 and Lemma 1, $\sigma[\Pi_{i=0}^{p-1}(x+i)^2+(x+i)+1]=\Pi_{i=0}^{p-1}[\sigma((x+i)^2+(x+i)+1)]=\Pi_{i=0}^{p-1}(x+j+i)(x+l+i)=(x^p-x)^2$ and we are done.■

Lemma 2. *For $p \geq 3$, the translates of $x^2+1 \in F_p[x]$ are distinct.*■

Theorem 20. *The polynomials $A=(x^p-x)^3$, $\sigma(A) \in F_p[x]$ form an amicable pair over F_p if and only if $p \equiv 3 (mod\ 8)$.*■

Theorem 21. *For $A=(x^p-x)^2$, the polynomials $B=A\sigma^2(A)$ and $\sigma(B)$ are an amicable pair over F_p if and only if $p \equiv$17,83,167,173,227,293,437,503,563,593,677,857,887, 923,1007,1097,1217,1223,1403,1427,1487,1517,1553,1613,1823,1847,2063,2147,2243,2273, 2327,2393,2477,2483,2537,2603,2747,2813,2873,2903,2987,3167,3197,3233,3317,3407,3527, 3533,3713,3737,3797,3827,3863,3923,4133,4157,4373,4457,4553,4583 (mod 4620).*

Proof. The result will follow from Theorem 22 and Theorem 23, as we now argue. The displayed polynomial A generates a 4-ring over F_p if and only if p satisfies the above congruence. In the proof of Theorem 23, the elements of the 4-ring generated by A are shown to be pairwise relatively prime. Hence by Theorem 22, the polynomials $B=A\sigma^2(A)$ and $\sigma(B)$ are amicable.■

Theorem 22. *Let $A_0 \in F_q[x]$ generate the even n-ring $A_0 \to A_1 \to \ldots \to A_{n-1} \to A_n = A_0$. If A_i, A_{i+2} relatively prime for $0 \le i < n$ and $B = \Pi_{k=1}^{\frac{n}{2}} A_{2k-1}$ and $C = \Pi_{k=0}^{\frac{n}{2}-1} A_{2k}$, then $(B, C)_{am}$.* ■

Example 10. For $A_0 = (x^{17} - x)^2 \in F_{17}[x]$, for $x_i = x + i$: $A_0 = (x^{17} - x)^2 \to \Pi_{i=0}^{16}(x_i^2 + x_i + 1) = A_1 \to \Pi_{i=0}^{16}(x_i^2 + x_i + 2) = A_2 \to \Pi_{i=0}^{16}(x_i^2 + x_i + 3) = A_3 \to \Pi_{i=0}^{16}(x_i^2 + x_i + 4) = \Pi_{i=0}^{16}[(x + 6 + i)(x + 12 + i)] = A_0$. ■

Theorem 23. The polynomial $A = (x^p - x)^2 \in F_p[x]$ generates a 4-ring over F_p if and only if $p \equiv$17,83,167,173,227,293,437,503,563,593,677,857,887,923,1007,1097,1217,1223, 1403,1427,1487,1517,1553,1613,1823,1847,2063,2147,2243,2273,2327,2393,2477,2483,2537, 2603,2747,2813,2873,2903,2987,3167,3197,3233,3317,3407,3527,3533,3713,3737,3797,3827, 3863,3923,4133,4157,4373,4457,4553,4583 (*mod* 4620).

Proof. If $p = 2$, then $(x^2 - x)^2 \to x^4 + x + 1 \to x^3(x + 1) \leftrightarrow x(x + 1)^3$. Thus $(x^2 - x)^2$ generates a $(1, 2)$-bracelet rather than a 4-ring. Hence assume $p \ge 3$. The discriminant of $\sigma(x^2) = x^2 + x + 1$ is $d = -3$. If $p = 3$, then $(x^3 - x)^2 \leftrightarrow (x^3 - x)^2$, so A is perfect over F_3. Hence assume $p \ge 5$. If $(\frac{-3}{p}) = 1$, then $x^2 + x + 1$ has distinct roots over F_p and factors as $x^2 + x + 1 = (x + l)(x + j)$. By Theorem 2 and Lemma 2, we have $\sigma((x^p - x)^2) = \Pi_{i=0}^{p-1}((x + i)^2 + (x + i) + 1) = \Pi_{i=0}^{p-1}(x + l + i)(x + j + i) = (x^p - x)^2$, so that A is perfect over F_p. Hence assume $p \ge 5$ and $(\frac{-3}{p}) = -1$, which occurs if and only if $p \equiv 5, 11 (mod\ 12)$. Then $x^2 + x + 1$ is prime over F_p. By Theorem 2 and Lemma 1, we have the canonical factorization $\sigma(x^p - x)^2 = \Pi_{i=0}^{p-1}((x + i)^2 + (x + i) + 1)$. The discriminant of $x^2 + x + 2$ is $d = -7$. Since $p \equiv 5, 11 (mod\ 12)$, then $p \ne 7$ so $p \ge 11$. By the proof of Theorem 19, if $(\frac{-7}{p}) = 1$ then $(A, \sigma(A))_{am}$ so that A does not generate a 4-ring. Hence assume $(\frac{-7}{p}) = -1$, which occurs if and only if $p \equiv 3, 5, 13, 17, 19, 27 (mod\ 28)$. Then $x^2 + x + 2$ is prime over F_p. By Theorem 2 and Lemma 1, $\sigma^2(A)$ has the canonical factorization $\sigma^2(A) = \Pi_{i=0}^{p-1}((x+i)^2+(x+i)+2)$, and $\sigma^3(A) = \Pi_{i=0}^{p-1}(\sigma((x+i)^2+(x+i)+2))$. Note that the discriminant of x^2+x+3 is $d = -11$. If $p = 11$, then $(A, \sigma(A))_{am}$ by Theorem 19, and A does not generate a 4-ring. If $(\frac{-11}{p}) = 1$, then $x^2 + x + 3$ has distinct roots over F_p and factors as $\sigma^3(x^2) = x^2 + x + 3 = (x + l)(x + j)$. Thus by Theorem 2 and Lemma 2, $\sigma^3(A) = \Pi_{i=0}^{p-1}((x + i)^2 + (x + i) + 3) = \Pi_{i=0}^{p-1}(x + l + i)(x + j + i) = (x^p - x)^2$ so that A generates a 3-ring over F_p. Hence assume $(\frac{-11}{p}) = -1$, so that $x^2 + x + 3$ is prime over F_p, which occurs if and only if $p \equiv 7, 13, 17, 19, 21, 29, 35, 39, 41, 43 (mod\ 44)$. By Theorem 2 and Lemma 1, $\sigma^3(A) = \Pi_{i=0}^{p-1}((x+i)^2+(x+i)+3)$ and $\sigma^4(A) = \Pi_{i=0}^{p-1}(\sigma((x+i)^2+(x+i)+3)) = \Pi_{i=0}^{p-1}((x + i)^2 + (x + i) + 4)$, and the discriminant of $x^2 + x + 4$ is $d = -15$. Assume that A generates a 4-ring over F_p. Then $\sigma^4(x^2) | (x^p - x)^2$. Thus $x^2 + x + 4$ factors. Hence $(\frac{-15}{p}) = 1$, which occurs if and only if $p \equiv 5, 7, 11, 13, 29, 37, 43, 59 (mod\ 60)$. Solving

$$\begin{cases} p \equiv 5, 11 (mod\ 12) \\ p \equiv 3, 5, 13, 17, 19, 27 (mod\ 28) \\ p \equiv 7, 13, 17, 19, 21, 29, 35, 39, 41, 42 (mod\ 44) \\ p \equiv 5, 7, 11, 13, 29, 37, 43, 59 (mod\ 60) \end{cases}$$

yields the desired congruence.

Conversely, let p satisfy the congruence. From earlier arguments: $A \to \Pi_{i=0}^{p-1}((x+i)^2+(x+i)+1) \to \Pi_{i=0}^{p-1}((x+i)^2+(x+i)+2) \to \Pi_{i=0}^{p-1}((x+i)^2+(x+i)+3) \to \Pi_{i=0}^{p-1}((x+i)^2+(x+i)+4)$. Since $p \equiv 5, 7, 11, 13, 29, 37, 43, 59 (mod\ 60)$ then $(\frac{-15}{p}) = 1$. Hence $\sigma^4(x^2)$ has distinct roots in F_p, say $\sigma^4(x^2) = (x+l)(x+j)$. By Theorem 2 and Lemma 1, $\sigma^4(A) = \Pi_{i=0}^{p-1}((x+i)^2+(x+i)+4) = \Pi_{i=0}^{p-1}(x+l+i)(x+j+i) = A$. ■

Corollary 24. *There exist 2-amicable pairs of polynomials over F_p for infinitely many primes p.*■

On mimicing Example 12 using amicable pairs from Table I, Theorems 19,20,21 and perfect polynomials displayed in or constructible from [2],[4],[8], there is evidence for this

Conjecture. *For all primes p and integers $k, d \geq 1$, there exist infinitely many $(A, B)_{k-am}$ over F_q, $q = p^d$.*■

References

1. Badawi, Ayman, *Non-Unitary Perfect Polynomials Over GF(p)*, unpublished master's thesis, Tennessee Technological University, 1988.
2. Beard, Jacob T. B., Jr., J. R. OConnell, and K. I. West, *Perfect Polynomials Over GF(q)*, vol. 8, 62, Atti. Acad. Naz. Lincei Rend. Cl. Sci. Fsi. Mat. Natur., 1977, pp. 283–291.
3. Beard, Jacob T. B., Jr., *Unitary Perfect Polynomials Over GF(q)*, vol. 8, 62, Atti. Acad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur., 1977, pp. 417–422.
4. Beard, Jacob T. B., Jr., A. T. Bullock, and M. S. Harbin, *Infinitely Many Perfect and Unitary Perfect Polynomials Over GF(q)*, vol. 8, 63, Atti. Acad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur., 1977, pp. 294–303.
5. Beard, Jacob T. B., Jr., and M. S. Harbin, *Non-splitting Unitary Perfect Polynomials Over GF(q)*, vol. 8, 66, Atti. Acad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur., 1979, pp. 179–185.
6. Beard, Jacob T. B., Jr., J. K. Doyle, and K. I. Mandelberg, *Square-Separable Primes and Unitary Perfect Polynomials*, vol. 8, 68, Atti. Acad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur., 1980, pp. 397–401.
7. Beard, Jacob T. B., Jr., *Bi-Unitary Perfect Polynomials Over GF(q)*, vol. IV, CIL, Annali di Mathematica Pura ed Applicata, 1987, pp. 61–68.
8. Beard, Jacob T. B., Jr., *Perfect Polynomials Revisited*, Publ. Math. Debrecen, 38, 1991, pp. 5–12.
9. Beard, Jacob T. B., Jr., and K. I. West, *Factorization Tables for GF[q,x]*, unpublished, 1973.
10. Canaday, E. F., *The Sum of the Divisors of a Polynomial*, Duke. Math. J., 7, 1941, pp. 721–737.
11. Clifford, A. H. and G. B. Preston, *Algebraic Theory of Semigroups*, vol. 1, American Mathematical Society, 1961.
12. Dickson, L. E., *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901; Dover Publications, New York, 1958.
13. Harary, Frank, *Graph Theory*, Addison-Wesley, Reading, 1969.
14. Higgins, Peter M., *Techniques of Semigroup Theory*, Oxford University Press, 1992.
15. Link, Martye Leanne, *Iterated Sums of Polynomial Divisors Over GF(p)*, unpublished master's thesis, Tennessee Technological University, 1995.
16. Long, A. F., Jr., *Factorization of Irreducible Polynomials over a Finite Field with the Substitution $x^{p^r} - x$ for x*, Duke Math. J., 40, 1973, pp. 63–76.
17. OConnell, James R., Jr., *Perfect Polynomials Over GF(p)*, unpublished master's thesis, University of Texas at Arlington, 1974.