

Perfect Polynomials over \mathbb{F}_3

Luis H. Gallardo ¹ and Olivier Rahavandrainy

Mathematics, University of Brest
6, Avenue Le Gorgeu, C.S. 93837
29238 Brest Cedex 3, France
luisgall@univ-brest.fr, rahavand@univ-brest.fr

Abstract

A perfect polynomial over the ternary field \mathbb{F}_3 is a monic polynomial $A \in \mathbb{F}_3[x]$ that equals the sum of all its monic divisors. If $\gcd(A, x^3 - x) = 1$ then we call A odd. We prove the nonexistence of odd perfect polynomials with 3 prime divisors, i.e., of the form $A = P^a Q^b R^c$ where P, Q, R are distinct irreducible monic polynomials over \mathbb{F}_3 . It follows from previous work of Beard et al. a characterization of all perfect polynomials with 3 prime factors over \mathbb{F}_3 .

Mathematics Subject Classification: 11T55, 11T06

Keywords: Sum of divisors, polynomials, finite fields, characteristic 3.

1 Introduction

Let p be a prime number. For a monic polynomial $A \in \mathbb{F}_p[x]$ let

$$\sigma(A) = \sum_{d|A, d \text{ monic}} d$$

be the sum of all monic divisors of A . Let us also call $\omega(A)$ the number of distinct monic prime (irreducible) polynomials that divide A . These functions are multiplicative, a fact that shall be used many times without more reference in the rest of the paper. A perfect polynomial A is a monic polynomial that divides $\sigma(A)$ or equivalently it is a polynomial A such that $\sigma(A) = A$.

¹Corresponding author

In all the paper we shall assume that “a polynomial” means a monic polynomial.

The notion of perfect polynomial (over \mathbb{F}_2) was introduced by Canaday [1], the first doctoral student of Leonard Carlitz. Later in the seventies Beard et al. (see [2]) and then Beard in a complementary paper (see [3]) characterized the splitting perfect polynomials over \mathbb{F}_p i.e., the polynomials that have a root in \mathbb{F}_p . We call these polynomials even (and the others odd) since we may think $x^p - x \in \mathbb{F}_p[x]$ as being the analogue of $p \in \mathbb{Z}$. Little is known about the odd perfect polynomials:

A simple congruence argument shows that an odd perfect polynomial in $\mathbb{F}_2[x]$ must be a perfect square. Also trivially there is no odd perfect polynomial over \mathbb{F}_2 with $\omega(A) = 1$. Canaday [1, Theorem 17] proved the inexistence of odd perfect polynomials with two prime factors, i.e., with $\omega(A) = 2$.

Recently, [6], we proved the inexistence of odd perfect polynomials over \mathbb{F}_2 with $\omega(A) = 3$.

Recently also, (see [7]) we proved the inexistence of odd perfect polynomials over \mathbb{F}_2 with $\omega(A) = 4$.

A perfect polynomial over \mathbb{F}_3 must have a number of minimal prime divisors that is a multiple of 3, (see Lemma 2.9) so trivially there is no perfect polynomials over \mathbb{F}_3 with 1 or 2 prime factors.

The object of this paper is to prove that there is no odd perfect polynomials over \mathbb{F}_3 with $\omega(A) = 3$, (see Theorem 2.10).

In order to do that we establish a variant in $\mathbb{F}_3[x]$ of some lemmata of Canaday for $\mathbb{F}_2[x]$ (see [1]). This may have its own interest and it is done in the next section.

By contrast with the integer case, observe that first Peirce in 1832 [8] and then Servais [10] and Sylvester [11] in 1888 already proved that every odd perfect number requires at least four prime factors.

In our time, (e.g.) this is proposed as a two starred exercise in [9, exercise 32, p. 232].

2 Some useful facts

We denote, as usual by \mathbb{N} the set of nonnegative integers. The first seven lemmata below are an analogue in characteristic 3 of Canaday's results [1, Lemma 5, Lemma 6]. They give (roughly) some information about the prime factorization of $1 + \dots + P^n$ for appropriate polynomials P .

The first four lemmata are the analogue (including information for all possible values of the exponent) in characteristic 3 of [4, Lemma 2.1]:

Lemma 2.1

Let \mathbb{F} be a perfect field of characteristic 3. Let $n, m \in \mathbb{N}$ be two non-negative integers. Let $P, Q \in \mathbb{F}[x]$ be two non constant polynomials, i.e., $P, Q \notin \mathbb{F}$. Assume that one has:

$$\sigma(P^{3n}) = 1 + \dots + P^{3n} = Q^m.$$

Then $m \in \{0, 1\}$.

Lemma 2.2

Let \mathbb{F} be a perfect field of characteristic 3. Let $n, m \in \mathbb{N}$ be two non-negative integers. Let $P, Q \in \mathbb{F}[x]$ be two non constant polynomials, i.e., $P, Q \notin \mathbb{F}$. Assume that one has:

$$\sigma(P^{3n+1}) = 1 + \dots + P^{3n+1} = Q^m.$$

Then either $m \in \{0, 1\}$ or

$$n = 0 \text{ and } \deg(P) > \deg(Q).$$

Lemma 2.3

Let \mathbb{F} be a perfect field of characteristic 3. Let $n, m \in \mathbb{N}$ be two non-negative integers. Let $Q \in \mathbb{F}[x]$ be a non constant polynomials, i.e., $Q \notin \mathbb{F}$. Assume that $P \in \mathbb{F}[x]$ is a prime such that

$$\sigma(P^{3n+1}) = 1 + \dots + P^{3n+1} = Q^m.$$

Then

$$m = 1.$$

Lemma 2.4

Let \mathbb{F} be a perfect field of characteristic 3. Let $n, m \in \mathbb{N}$ be two non-negative

integers. Let $P, Q \in \mathbb{F}[x]$ be two non constant polynomials, i.e., $P, Q \notin \mathbb{F}$. Assume that $\gcd(Q, Q') = 1$ (e.g. assume that Q is prime) and that

$$\sigma(P^{3n+2}) = 1 + \dots + P^{3n+2} = Q^m.$$

Then $m \in \{-1, 1\} \pmod{3}$ and

$$Q \text{ divides } P - 1.$$

Proof of the four lemmata: In order to prove Lemma 2.1 we rewrite

$$1 + \dots + P^{3n} = Q^m \tag{1}$$

as

$$P^{3n+1} - 1 = (P - 1)Q^m. \tag{2}$$

If $n = 0$ then from (2) we get $m = 0$, thus we may assume that $n \geq 1$. We can also rewrite (1) as:

$$(1 - P)^2(1 + \dots + P^{n-1})^3 + P^{3n} = Q^m \tag{3}$$

If 3 divides m then the equation (3) implies that P is a cube so that by taking enough cubic roots if necessary in both sides of (3) we may assume that $m \not\equiv 0 \pmod{3}$. Thus $P' \neq 0$ and $m \geq 1$. By taking derivatives in both sides of (2) we get

$$P^{3n} P' = Q^{m-1} (P'Q + m(P - 1)Q'). \tag{4}$$

From (1) $\gcd(P, Q) = 1$, so we get from (4) that Q^{m-1} divides P' Thus

$$(m - 1) \deg(Q) < \deg(P).$$

But, by taking degrees on both sides of (1) we have:

$$m \deg(Q) = 3n \deg(P).$$

So,

$$3n \deg(P) - \frac{3n}{m} \deg(P) < \deg(P)$$

i.e.:

$$n(m - 1) < \frac{m}{3}$$

But $n \geq 1$, thus

$$(m - 1) < \frac{m}{3}$$

i.e.,

$$2m < 3$$

so that $m = 1$. This proves the lemma.

The proof of Lemma 2.2 when $n \geq 1$ is similar. We assume then $n = 0$ and $m \notin \{0, 1\}$. Then by taking degrees on both sides of $1 + P = Q^m$ we get immediately that

$$\deg(P) = m \deg(Q) > \deg(Q),$$

thereby completing the proof of the lemma.

To prove Lemma 2.3 observe that if $n \geq 1$ then it follows from Lemma 2.2 that $m \leq 1$. If $m = 0$ then $P \in \mathbb{F}$ that is impossible. So $m = 1$. It remains the case $n = 0$: From

$$1 + P = Q^m \tag{5}$$

we get

$$P = (Q - 1)(Q^{m-1} + \dots + 1).$$

But, P is prime, so either $Q - 1 = 1$ that is impossible or $Q - 1 = P$. Thus $\deg(Q) = \deg(P)$. It follows then from (5) that

$$m = 1.$$

This proves Lemma 2.3 .

In order to prove Lemma 2.4 we rewrite

$$1 + \dots + P^{3n+2} = Q^m \tag{6}$$

as

$$P^{3n+3} - 1 = (P - 1)Q^m. \tag{7}$$

As before we rewrite (6) as:

$$(P - 1)^2(1 + \dots + P^n)^3 = Q^m \tag{8}$$

If 3 divides m then equation (8) implies that P is a cube so that by taking enough cubic roots if necessary in both sides of (8) we may assume that $m \neq 0$

(mod 3). Thus $P' \neq 0$ and $m \geq 1$. By taking derivatives in both sides of (7) we get

$$0 = P'Q + m(P - 1)Q'. \quad (9)$$

From hypothesis $\gcd(Q, Q') = 1$. It follows that

$$Q \text{ divides } P - 1.$$

This finishes the proof of our first four lemmata in the section.

The following three lemmata are the analogue in characteristic 3 of [1, Lemma 6]:

Lemma 2.5

Let \mathbb{F} be a perfect field of characteristic 3. Let $P, Q \in \mathbb{F}[x]$ be irreducible. Let $C \in \mathbb{F}[x]$ be a polynomial with $\gcd(Q, C) = 1$. Let $n, m \in \mathbb{N}$ be two non-negative integers. Let $r \in \{0, 1\}$. If

$$\sigma(P^{3n+r}) = 1 + \dots + P^{3n+r} = Q^m C.$$

Then

(a) If $m > 1$ then $\deg(C) > 0$.

(b) If $m \geq 3$ then

$$\deg(P) > 3 \deg(Q).$$

(c) If $m = 2$ then

$$\deg(P) > \deg(Q).$$

(d) If $n = 0$, $m \geq 2$ and $r = 1$ then

$$\deg(P) > 2 \deg(Q).$$

Lemma 2.6

Let \mathbb{F} be a perfect field of characteristic 3. Let $P, Q \in \mathbb{F}[x]$ be such that P, Q are irreducible. Let $C \in \mathbb{F}[x]$ be a polynomial with $\gcd(Q, C) = 1$.

Let $n, m \in \mathbb{N}$ be two non-negative integers. Assume that

$$\sigma(P^{3n+2}) = 1 + \dots + P^{3n+2} = Q^m C$$

and that

$$Q \text{ divides } P - 1.$$

Then $m > 1$.

Moreover, if $n \equiv -1 \pmod{3}$ then $m > 4$. Furthermore, if m is a multiple of 3 then:

(1) $Q \mid \gcd(P', P'')$ so that

$$\deg(P) > \deg(Q) + 1.$$

(2) if $n \equiv -1 \pmod{3}$ then $m \geq 9$.

(3) if $n \in \{0, 1\} \pmod{3}$ then $6 \mid m$ and

$$\deg(P) \geq 3 \deg(Q).$$

Lemma 2.7

Let \mathbb{F} be a perfect field of characteristic 3. Let $P, Q \in \mathbb{F}[x]$ be such that P, Q are irreducible. Let $C \in \mathbb{F}[x]$ be a polynomial with $\gcd(Q, C) = 1$.

Let $n \in \mathbb{N}$ be a non-negative integer. Let $m > 0$ be a positive integer. Assume that:

$$\sigma(P^{3n+2}) = 1 + \cdots + P^{3n+2} = Q^m C$$

and that

$$Q \nmid P - 1$$

Q does not divide $P - 1$.

Then C is not a cube in $\mathbb{F}[x]$, so that $\deg(C) > 0$. Moreover:

$n > 0$, and $m \geq 3$ is a multiple of 3.

Furthermore:

$$Q^{\frac{m}{3}} \text{ divides } 1 + \cdots + P^n.$$

Proof of the three lemmata: Observe that Lemma 2.5 (a) follows from Lemma 2.1 and from Lemma 2.3. We prove parts (b) and (c) only in the case $r = 0$, the proof in the case $r = 1$ is similar. From

$$1 + \cdots + P^{3n} = Q^m C$$

we get

$$P^{3n+1} - 1 = (P - 1)Q^m C \tag{10}$$

Then by taking derivatives in both sides of (10) we get

$$P^{3n}P' = Q^{m-1}(P'QC + (P-1)(mQ'C + QC')),$$

so that (observe that $\gcd(P, Q) = 1$)

$$Q^{m-1} \mid P'. \text{ Moreover } Q^m \mid P' \text{ provided } m \equiv 0 \pmod{3}.$$

By observing that $\deg(P) > \deg(P')$, we see that (b) and (c) follows immediately.

It remains to prove (d): By part (a) we have $\deg(C) > 0$. The result follows by taking degrees in both sides of the equation:

$$1 + P = Q^m C.$$

This proves Lemma 2.5.

Now we prove Lemma 2.6. The first hypothesis may be written:

$$(1 + \dots + P^n)^3(P-1)^2 = Q^m C \tag{11}$$

We see that the exponent e of Q in the left hand side of (11) exceeds 1. So $m > 1$. Assuming $n \equiv -1 \pmod{3}$ it is also clear from (11) that $m = e \geq 3 + 2 > 4$.

Assume now that m is a multiple of 3. Writing the hypothesis (11) in the form

$$P^{3n+3} - 1 = (P-1)Q^m C, \tag{12}$$

we get by taking derivatives in both sides of (12):

$$0 = P'C + (P-1)C' \tag{13}$$

from which, by using $Q \mid P-1$ and $\gcd(Q, C) = 1$ we see that

$$Q \mid P'.$$

By differentiating both sides of (13) we get

$$0 = P''C - P'C' + (P-1)C''. \tag{14}$$

It follows from (14) that

$$Q \mid P''$$

so that Q divides $\gcd(P', P'')$ and

$$\deg(P) > \deg(P'') + 1 \geq \deg(Q) + 1.$$

Therefore we proved (1). Now we prove the results (2) and (3) : We take $n \equiv -1 \pmod{3}$. Then Q divides $1 + \dots + P^n$ since $P \equiv 1 \pmod{Q}$. Assume that Q appears exactly a times in $1 + \dots + P^n$ and b times in $P - 1$. From (11) we obtain

$$m = 3a + 2b$$

so, $b \geq 1$ is a multiple of 3. It follows that

$$m \geq 3 + 6 = 9.$$

Assume now that $n \in \{0, 1\} \pmod{3}$. It follows that $\gcd(Q, 1 + \dots + P^n) = 1$ since $P \equiv 1 \pmod{Q}$, so that we obtain from (11):

$$Q^m \parallel (P - 1)^2. \quad (15)$$

In particular m is even so that $6 \mid m$. From (15) we get immediately:

$$\deg(P) \geq \frac{m}{2} \deg(Q) \geq 3 \deg(Q).$$

This finishes the proof of Lemma 2.6.

Assume now that $Q \nmid (P - 1)$. Since $\gcd(Q, C) = 1$ we get from (11) that $n > 0$ and:

$$Q^m \parallel (1 + \dots + P^n)^3 \quad (16)$$

so that m is a multiple of 3. From the same equation (11) we obtain that C is not a cube in $\mathbb{F}[x]$. For if C it is indeed a cube then from (11) we deduce that P is a cube. But this is impossible. We can also see directly that $\deg(C) > 0$ from Lemma 2.4. We get immediately from (16) that

$$Q^{\frac{m}{3}} \mid 1 + \dots + P^n.$$

thereby finishing the proof of the three lemmata.

The following lemma is useful:

Lemma 2.8

Let $P \in \mathbb{F}_3[x]$ be an odd prime, i.e., an irreducible polynomial of degree > 1 . Then at least one of $P + 1$ and $P - 1$ is composite.

Proof: Assume that $P - 1$ and $P + 1$ are both prime. Since P is odd we have $P(0) \neq 0$ so that $P(0)^2 = 1$. Similarly we get $(P - 1)(0)^2 = 1$ and $(P + 1)(0)^2 = 1$. So, we get the contradiction:

$$0 = (P(0)^2 - 1)^2 = (P^2 - 1)^2(0) = (P - 1)(0)^2(P + 1)(0)^2 = 1.$$

This proves the lemma.

The following crucial lemma is the case $p = 3$ of [6, Lemma 2.3] or [5, Lemma 2.5] that improves a result of Beard et al., [2, Theorem 7]:

Lemma 2.9

Let $A \in \mathbb{F}_3[x]$ be a perfect polynomial. Then the number of minimal primes of A , i.e., the number of prime divisors of A having minimal degree, is a multiple of 3.

The object of the paper is to prove our main result:

Theorem 2.10

There is no odd perfect polynomials $A \in \mathbb{F}_3[x]$ with three prime divisors, i.e., of the form $A = P^a Q^b R^c$ where P, Q, R are distinct irreducible polynomials of degree > 1 over \mathbb{F}_3 and a, b, c are positive integers.

We get immediately:

Corollary 2.11 *The only perfect polynomials over \mathbb{F}_3 with $\omega(A) \leq 3$ are*

$$0, (x^3 - x)^{3^n - 1}, (x^3 - x)^{2 \cdot 3^n - 1},$$

where $n \geq 0$ is a non-negative integer.

Proof: It follows from Theorem 2.10 and from theorems [2, Theorem 5] and [3, Theorem 1].

3 Proof of Theorem 2.10

The general strategy of the proof is as follows: Let A be an odd perfect polynomial with $\omega(A) = 3$. Let P, Q, R be the distinct primes that divide A . Set

$\delta_1 = \deg(P)$, $\delta_2 = \deg(Q)$, $\delta_3 = \deg(R)$. From Lemma 2.9 we see that all these degrees are equal to, say, $\delta > 0$:

$$\delta_1 = \delta_2 = \delta_3 = \delta \geq 1.$$

Moreover, we may assume that for some integers $r_1, r_2, r_3 \in \{0, 1, 2\}$ and for some non-negative integers a, b, c with

$$3a + r_1, 3b + r_2, 3c + r_3 > 0,$$

we have:

$$A = P^{3a+r_1} Q^{3b+r_2} R^{3c+r_3} = \sigma(A). \quad (17)$$

We shall prove that this is impossible. In order to do that we rewrite the condition in (17) (by using the multiplicativity of σ) as a system:

$$\text{E1: } \sigma(P^{3a+r_1}) = Q^{b_1} R^{c_1},$$

$$\text{E2: } \sigma(Q^{3b+r_2}) = P^{a_1} R^{c_2},$$

$$\text{E3: } \sigma(R^{3c+r_3}) = P^{a_2} Q^{b_2}.$$

in which the exponents in the right hand side are non-negative numbers.

- (a) We observe that a single equation in which $r_i = 0$ is quickly proved impossible. By symmetry, it remains only four cases to study. Each is considered in his own section.
- (b) Contradictions will be built for each of these four cases by using our above lemmata.

4 Case 1: Some r_i is zero

This is the simplest case. Take, e.g., $r_1 = 0$. By applying Lemma 2.5 to the equation E1: $\sigma(P^{3a}) = Q^{b_1} R^{c_1}$, we get immediately $b_1, c_1 \in \{0, 1\}$. So, by taking degrees on both sides of E1 (and by cancelling the common degree δ) we get the contradiction:

$$3 \leq 3a = b_1 + c_1 \leq 2.$$

5 Case 2: $r_1 = r_2 = r_3 = 2$

Our system is then:

$$\text{E1: } \sigma(P^{3a+2}) = Q^{b_1} R^{c_1},$$

$$\text{E2: } \sigma(Q^{3b+2}) = P^{a_1} R^{c_2},$$

$$\text{E3: } \sigma(R^{3c+2}) = P^{a_2} Q^{b_2}.$$

By symmetry, we may divide the case into two parts depending on the value of c_1 :

5.1 subcase 2A: $c_1 = 0$

Equation E1 is now: $1 + \dots + P^{3a+2} = Q^{b_1}$. It follows from Lemma 2.4 that $Q \mid P - 1$ so that (remember that $\deg(P) = \deg(Q)$)

$$Q = P - 1. \tag{18}$$

Now we consider equation E2. If P divides $Q - 1$ then $P = Q - 1$. But this together with (18) implies the contradiction

$$P = P + 1.$$

Similarly, if R divides $Q - 1$ we get $R = Q - 1$ so that by (18) the three polynomials $Q, Q - 1 = R, Q + 1 = P$ are odd primes. This is impossible by Lemma 2.8.

Thus, $R \nmid Q - 1$ so that by Lemma 2.7 applied to E2 we get that c_2 is a multiple of 3. But this contradicts the fact that the exponent of R in $A = \sigma(A)$ equals $3c + 2 = c_2$.

5.2 subcase 2B: $c_1 > 0$ and $b_1 > 0$

Observe that P, Q, R have the same degree so that we cannot have simultaneously $Q \mid P - 1$ and $R \mid P - 1$. On the other hand $\sigma(P^{3a+2})$ is not a cube. So from Lemma 2.7 applied to E1, we get that the only possibility that E1 holds is that exactly one of Q, R , say Q divides $P - 1$. We have then

$$Q = P - 1. \tag{19}$$

Observe that the previous subcase 5.1 says that we can always assume that all exponents on the right hand side of our equations E1, E2, E3 are both

positive. This allow us to proceed similarly: From Lemma 2.7 applied to E2, we get that exactly one of P, R , divides $Q - 1$. If $P \mid Q - 1$ then $P = Q - 1$ that contradicts (19). If $R \mid Q - 1$ then $R = Q - 1$ so that $Q - 1 = R, Q, Q + 1 = P$ are three odd primes. This contradicts Lemma 2.8.

6 Case 3: $r_1 = r_2 = 2, r_3 = 1$

Our system is then:

$$\text{E1: } \sigma(P^{3a+2}) = Q^{b_1} R^{c_1},$$

$$\text{E2: } \sigma(Q^{3b+2}) = P^{a_1} R^{c_2},$$

$$\text{E3: } \sigma(R^{3c+1}) = P^{a_2} Q^{b_2}.$$

By Lemma 2.5 (d) applied to E3, we get $a_2, b_2 \in \{0, 1\}$. Assume that $c \neq 0$. Then we get the contradiction

$$4 \leq 3c + 1 = a_2 + b_2 \leq 2.$$

So $c = 0$. This implies by comparing degrees on both sides of E3 that

$$1 = a_2 + b_2, \tag{20}$$

while comparing the exponent of R in both sides of $A = \sigma(A)$ gives:

$$1 = c_1 + c_2. \tag{21}$$

By switching if necessary P and Q it suffices to study the subcase: $c_1 = 1$ (so $c_2 = 0$): From Lemma 2.4 applied to E2, we get $P \mid Q - 1$, i.e., $P = Q - 1$. Observe that the exponent of R in E1 is $1 > 0$ that is not a multiple of 3. Then from Lemma 2.7 applied to E1, we get $R \mid P - 1$, i.e., $R = P - 1$. So, $P, P - 1 = R, P + 1 = Q$ are three odd primes. This contradicts Lemma 2.8.

7 Case 4: $r_1 = 2, r_2 = r_3 = 1$

Our system is then:

$$\text{E1: } \sigma(P^{3a+2}) = Q^{b_1} R^{c_1},$$

$$\text{E2: } \sigma(Q^{3b+1}) = P^{a_1} R^{c_2},$$

$$\text{E3: } \sigma(R^{3c+1}) = P^{a_2}Q^{b_2}.$$

Observe that from Lemma 2.5 applied to E3, we get $a_2, b_2 \in \{0, 1\}$. Similarly, from Lemma 2.5 applied to E2, we get $a_1, c_2 \in \{0, 1\}$. This implies by comparing degrees in both sides of equations E3 and E2:

$$3c + 1 = a_2 + b_2 \leq 2, \quad \text{and} \quad 3b + 1 = a_1 + c_2 \leq 2$$

so that

$$b = 0 \quad \text{and} \quad c = 0.$$

and

$$1 = a_2 + b_2, \quad 1 = a_1 + c_2.$$

By comparing the exponents of P in both sides of $A = \sigma(A)$ we get

$$3a + 2 = a_1 + a_2 \leq 2$$

so $a = 0$ also, and

$$2 = a_1 + a_2, \quad \text{i.e., } a_1 = 1 = a_2.$$

Thus,

$$b_2 = c_2 = 0.$$

The latter two equations of the system become:

$$\text{E2: } 1 + Q = P,$$

$$\text{E3: } 1 + R = P.$$

This is impossible.

8 Case 5: $r_1 = r_2 = r_3 = 1$

Our system is then:

$$\text{E1: } \sigma(P^{3a+1}) = Q^{b_1}R^{c_1},$$

$$\text{E2: } \sigma(Q^{3b+1}) = P^{a_1}R^{c_2},$$

$$\text{E3: } \sigma(R^{3c+1}) = P^{a_2}Q^{b_2}.$$

First of all, observe that from Lemma 2.5 applied to each equation of the system, we get that all exponents in the right hand side of our three equations

are in $\{0, 1\}$. Thus, by comparing degrees in both sides of each equation we get as before $a = b = c = 0$ and

$$1 = b_1 + c_1, \quad 1 = a_1 + c_2, \quad 1 = a_2 + b_2.$$

Thus, by comparing exponents of P, Q, R in both sides of $A = \sigma(A)$ we get

$$1 = a_1 + a_2, \quad 1 = b_1 + b_2, \quad 1 = c_1 + c_2.$$

By symmetry we may assume that $b_1 = 1$ and $c_1 = 0$. So, $b_2 = 0$ and $c_2 = 1$ so that $a_1 = 0$. We have then

$$\text{E1: } 1 + P = Q, \text{ and E2: } 1 + Q = R$$

$$1 + P = Q.$$

In E2, $1 + Q = P$ or $1 + Q = R$. In the first case we get the contradiction $Q+1 = Q-1$, while in the latter case we get that so that $Q, Q-1 = P, Q+1 = R$ are three odd primes. This contradicts Lemma 2.8.

This proves the theorem.

References

[1]

E. F. CANADAY, *The sum of the divisors of a polynomial*, Duke Math. Journal **8** (1941), 721 – 737.

[2]

T. B. BEARD JR, JAMES. R. OCONNELL JR, KAREN I. WEST, *Perfect polynomials over $GF(q)$* , Rend. Accad. Lincei **62** (1977), 283 – 291.

[3]

J. T. B. BEARD JUN., *Perfect polynomials revisited*, Publ. Math. **38**, No. 1/2 (1991), 5 – 12.

[4]

L. GALLARDO, O. RAHAVANDRAINNY, *On perfect polynomials over \mathbb{F}_4* , Portugaliae Mathematica **62 - Fasc. 1** (2005), 109– 122.

[5]

L. GALLARDO, O. RAHAVANDRAINY, *Perfect polynomials over \mathbb{F}_4 with less than five prime factors*, Portugaliae Mathematica **64 - Fasc. 1** (2007), 21–38.

[6]

L. H. GALLARDO, O. RAHAVANDRAINY, *Odd perfect polynomials over \mathbb{F}_2* , J.T.N.B. **19** (2007), 167–176.

[7]

L. H. GALLARDO, O. RAHAVANDRAINY, *There is no odd perfect polynomial over \mathbb{F}_2 with four prime factors*, Preprint.

[8]

BENJAMIN PEIRCE, *On perfect numbers*, New York Math. Diary **2, XIII** (1832), 267 – 277.

[9]

K. H. ROSEN, *Elementary number theory and its applications. 3rd ed.*, Addison-Wesley Publishing Company , Reading, MA, 1993.

[10]

C. SERVAIS, *Sur les nombres parfaits*, Mathesis **8** (1888), 135.

[11]

J. J. SYLVESTER, *Sur les nombres parfaits*, Comptes Rendus Paris **106** (1888), 403 – 405.

Received: November 21, 2007