Acta Math. Univ. Comenianae
Vol. LXXXV, 2 (2016), pp. 261–275

THERE ARE FINITELY MANY EVEN PERFECT POLYNOMIALS OVER $\mathbb{F}_p$ WITH $p+1$ IRREDUCIBLE DIVISORS

L. H. GALLARDO AND O. RAHAVANDRAINY

ABSTRACT. For a fixed prime number p, we give necessary conditions for the existence of products of $p+1$ distinct monic irreducible polynomials in one variable over the finite field $\mathbb{F}_p$, each raised to an arbitrary positive power. The polynomials are *even perfect* polynomials; i.e., they have at least one root in $\mathbb{F}_p$ and are equal to the sum of all their monic divisors. As a consequence, we prove that the set of such polynomials is *finite*, and if $q = \frac{p-1}{2}$ is also prime, so that q is a Sophie Germain prime and p is a safe prime, then it is empty. This is the first known finiteness result for perfect polynomials. We might consider it as an analogue of Dickson's result that proves the finiteness of the set of odd perfect numbers with a fixed number of distinct prime divisors, each raised to an arbitrary positive power.

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 (1 and A included). The restriction to monic polynomials is necessary since the sum of all divisors of A with a given degree is zero. Observe that A and $\sigma(A)$ have the same degree. Let us call $\omega(A)$ the number of distinct monic irreducible polynomials that divide A. The function σ is multiplicative on co-prime polynomials while the function ω is additive (on co-prime polynomials), a fact that is used many times without more reference in the rest of the paper.

Throughout the paper, we assume that "a polynomial" means a monic polynomial and the notion of irreducibility is defined over the ground field $\mathbb{F}_p$.

We say that a polynomial A is *perfect* if $\sigma(A) = A$. It is *even* if it has at least one root in $\mathbb{F}_p$, and *odd* if it is not even (see [**10**] for more details).

The first and most important results about perfect polynomials appear in the work of Canaday [**4**] and Beard et al. ([**1**], [**2**]). We obtained (see [**7**], [**8**], [**9**], [**10**] and the references therein) some results about even, odd or splitting perfect

Received June 5, 2015; revised September 27, 2015.
2010 *Mathematics Subject Classification.* Primary 11T55, 11T06.
Key words and phrases. Perfect polynomials; finite fields; characteristic p.

polynomials that generalize the work of Canaday and Beard et al.. For an odd prime p, we began [**10**] to study, perfect polynomials over $\mathbb{F}_p$ with $p+1$ irreducible factors, since the case $p=2$ was already resolved in ([**4**, Theorem 9], [**8**, Theorem 3.1]). Moreover, we completely solved the case $p=3$ (see [**10**, Theorem 1.1 and Theorem 1.2]). In this paper, we substantially improve [**10**] for the case of even perfect polynomials and get the following result.

Theorem 1.1. *Let p be an odd prime number. Then the even perfect polynomials $A(x)$ over $\mathbb{F}_p$ with $\omega(A(x)) = p+1$ irreducible factors form a finite set (which may be empty). Then for some $\xi \in \mathbb{F}_p$,*

$$A(x+\xi) = \prod_{j=1}^{p} (x+j)^{N_j - 1} \cdot Q,$$

where $N_p \nmid p-1$, $N_j \mid p-1$ for any $j \neq p$. Moreover, the N_j's and Q also satisfy one of the following conditions:

(1) *$N_p = 4$, $Q = 1+x^2$, $N_{j_1} = 2$ for a unique j_1, $N_j \geq 3$ if $j \neq j_1$, $p \equiv 3 \mod 8$,*
(2) *N_p is an odd prime, $Q = \sigma(x^{N_p-1})$ is irreducible, $1+Q$ splits over $\mathbb{F}_p$, $N_{j_1} = N_p - 1$ for a unique j_1, $3 \leq N_p \leq \frac{p-3}{2}$, $N_j > N_p$ if $j \notin \{j_1, p\}$,*
(3) *N_p is an odd prime, $Q = \sigma(x^{N_p-1})$ is irreducible, $1+Q$ splits over $\mathbb{F}_p$, $5 \leq N_p \leq \frac{p-3}{2}$, $N_j > N_p$ for any $j \neq p$.*

Remark 1.2. In (1) (resp., in (2) with $N_p = 3$), the irreducibility condition on Q and the splitting of $1+Q$ are equivalent to the congruence: $p \equiv 3 \mod 8$ (see Lemma 3.19) (resp. $p \equiv 2, 8$ or $11 \mod 21$). Moreover, if $p = 3$, our present result in (1) immediately implies our [**10**, Theorem 1.2].

Remark 1.3. The core of our proof of Theorem 1.1 (see Section 3) is to prove that the set of the N_j's above is finite.

Observe that for any given positive integer w, there are infinitely many polynomials $A \in \mathbb{F}_p[x]$ with $\omega(A) = w$, so potentially an infinity of perfect polynomials with $\omega(A) = w$ may exist. However, for example, if $p = 2$ and $w = 3$, ([**4**, Theorem 9], [**8**, Theorem 3.1]), we get exactly four polynomials:

$$x(x+1)^2(x^2+x+1), \qquad x^2(x+1)(x^2+x+1),$$
$$x^3(x+1)^4(x^4+x^3+1), \qquad x^4(x+1)^3(x^4+x^3+x^2+x+1).$$

If p is odd and $w = p$, we know only (see [**9**, Theorem 1.2]) a unique odd perfect polynomial $L \in \mathbb{F}_p[x]$. More precisely, one has $L = \prod_{a \in \mathbb{F}_p} ((x+a)^2 - 3/8)^2$, where $p \equiv 11,\ 17 \mod 24$. We do not know whether or not there are more odd perfect polynomials.

Nevertheless, albeit concerning the special case $w = p+1$, the finiteness result given by Theorem 1.1 is a new important result that might be considered as a kind of "analogue" to the Dickson's result [**5**] over the integers. No other finiteness results for perfect polynomials seem known. The best one that we obtained concerns only the exponents of the irreducible polynomials dividing odd perfect polynomials over $\mathbb{F}_p$ with $w = p$ (see [**9**, Theorem 1.1]).

We get (Corollary 1.4) a more precise result if p is a *safe* primedefined as a prime number of the form $2r+1$, where r is also a prime. In this case, the prime r is called a *Sophie Germain* prime. The sequence of safe primes is A005385 in the OEIS [**15**], whereas that of Sophie Germain primes is A005384 and begins

2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293.

A recent theoretical paper on Sophie Germain primes is [**14**]. Most papers on this subject are computational ones, e.g., [**6**], [**11**], [**17**]. It is believed that both sequences (Sophie Germain and safe primes) are infinite.

Our second main result is the following corollary.

Corollary 1.4. *If p is a safe prime, then there exists no even perfect polynomial over $\mathbb{F}_p$ with $p+1$ irreducible divisors.*

In (2) and (3) of Theorem 1.1, the only irreducible odd divisor $Q=\sigma(x^{N_p-1})$ of A must satisfy: $1+Q$ splits over $\mathbb{F}_p$. For a given polynomial, the splitting condition over $\mathbb{F}_p$, may be satisfied for infinitely many values of p as it is explained in a paper of J. P. Serre ([**16**, Theorem 1, part (a)]). But it is more difficult to find examples of irreducible Q's with the condition $1+Q$ splits over $\mathbb{F}_p$. However, this may occur. Indeed, one has

$$(x-1)(1+Q)=x^{N_p}+x-2,$$

so $1+Q$ splits if and only if $x^{N_p}+x-2$ splits. Below, we give some numerical values of N_p and p (obtained by Maple computations) for which this is possible. For instance, there are only four such primes $p<10^9$ when $N_p=11$.

N_p	5	5	5	5	7	7	11	11	11	11
p	227	313	467	613	8069	10601	220316791	239909909	435731447	758471447

2. Useful facts

By $\mathbb{N}$ (resp. by $\mathbb{N}^*$) as usual, we denote the set of nonnegative integers (resp., of positive integers). For a set Λ, we denote the cardinal of Λ by $\#\Lambda$.

For polynomials $A,B\in\mathbb{F}_p[x]$, we write $A^n\|B$ if $A^n\mid B$ but $A^{n+1}\nmid B$.

Definition 2.1. We say that a polynomial P is a *minimal irreducible divisor* of A if P is irreducible, P divides A and $\deg(P)\le\deg(R)$ for any irreducible divisor R of A.

Basic but important results are the following ones.

Lemma 2.2. *Let p be a prime number and $A\in\mathbb{F}_p[x]$ be a perfect polynomial. Then*

i) *for any $\xi\in\mathbb{F}_p$, $A(x+\xi)$ is also perfect,*

ii) *the number of minimal irreducible divisors of A is a multiple of p,*

iii) *if $\omega(A)=p+1$, then A may be written as*

$$A=P_1^{a_1}\cdots P_p^{a_p}\cdot Q^b,\ \text{where } a_j,b\in\mathbb{N}^* \ \text{ and } \ \deg(P_j)=\deg(P_1)<\deg(Q).$$

Proof. i) is obvious, ii) is [**7**, Lemma 2.5] and iii) follows from ii). □

We also recall some known necessary conditions on A (see [**10**, Theorem 1.1]) that we improve for A even.

Proposition 2.3. *Let p be an odd prime number. Let $A = P_1^{a_1} \cdots P_p^{a_p} Q^b$ be a perfect polynomial over $\mathbb{F}_p$ with $p+1$ irreducible factors and $\deg(Q) > \deg(P_j) = \deg(P_1)$ for any j. Then*

i) *A is even or at least one of the numbers a_j, $j \in \{1, \ldots, p\}$ is even,*

ii) *for at least one $j \in \{1, \ldots, p\}$, a_j is of the form $N_j p^{n_j} - 1$ with $N_j, n_j \in \mathbb{N}$, $N_j \geq 1$, $p \nmid N_j$ and $N_j \nmid p-1$,*

iii) *either $p \nmid b+1$, or $b \in \{p-1, 2p-1\}$ and $\deg(P_1) \mid \deg(Q)$.*

Notation 2.4. In the rest of the paper, we fix an odd prime number p. According to Lemma 2.2-iii) for an even perfect polynomial $A \in \mathbb{F}_p[x]$ with $\omega(A) = p+1$, we put

$$A = \prod_{i=1}^{p} P_i^{a_i} \cdot Q^b, \text{ where } P_i := x + i, \quad a_i, b \in \mathbb{N}^* \text{ and } \deg(Q) \geq 2,$$

$$a_i = N_i p^{n_i} - 1, \ b = M p^m - 1, \quad N_i, n_i, M, m \in \mathbb{N}, \quad N_i, M \geq 1, \quad p \nmid N_i, \ p \nmid M.$$

However, if a more precision is necessary, we sometimes write $x+i$ instead of P_i.

Remark 2.5. From the perfectness of A and the multiplicativity of σ, we get

$$\prod_{i=1}^{p} \sigma(P_i^{a_i}) \sigma(Q^b) = \sigma(A) = A = \prod_{i=1}^{p} P_i^{a_i} Q^b = \prod_{i=1}^{p} (x+i)^{a_i} Q^b. \tag{2.1}$$

In Section 3, we often use Lemma 2.6 and some properties of cyclotomic polynomials (for more details, see [**12**, Definition 2.44, Theorems 2.45 and 2.47]).

Lemma 2.6. ([**10**, Lemma 2.6]) *Let $p, N \in \mathbb{N}$ such that p is an odd prime and $p \nmid N$. Let $U \in \mathbb{F}_p[x]$ be an irreducible polynomial. If $\sigma(U^{N-1}) = Q_1^{c_1} \cdots Q_t^{c_t}$, where each Q_l is irreducible, $\gcd(U, Q_l) = 1$ and $\deg(U) \leq \deg(Q_l)$ for any l, then $c_l \in \{0, 1\}$ for any l.*

By $\mathcal{Q}_N(x) \in \mathbb{F}_p[x]$, we denote the Nth cyclotomic polynomial over $\mathbb{F}_p$ for a positive integer N not divisible by p.

Lemma 2.7.

i) *One has $x^N - 1 = \prod_{d \mid N} \mathcal{Q}_d(x)$ and $\sigma(x^{N-1}) = \prod_{d \mid N, \ d \neq 1} \mathcal{Q}_d(x)$.*

ii) *The polynomial $\mathcal{Q}_N(x)$ in $\mathbb{F}_p[x]$ factorizes into $\dfrac{\varphi(N)}{d}$ distinct monic irreducible polynomials of the same degree d, where φ is the Euler totient function and d is the least positive integer such that $p^d \equiv 1 \mod N$.*

Immediate consequences follow.

Corollary 2.8.

i) *If $d \neq v$ are divisors of N, then $\gcd(\mathcal{Q}_d(x), \mathcal{Q}_v(x)) = 1$.*

ii) *The polynomial* $\mathcal{Q}_N(x)$ *splits over* $\mathbb{F}_p$ *if and only if* $N \mid p-1$.

iii) *If* $\mathcal{Q}_N(x)$ *is reducible and does not split over* $\mathbb{F}_p$, *then* $\mathcal{Q}_N(x)$ *has at least two irreducible odd factors.*

iv) *If* N *is prime, then* $\mathcal{Q}_N(x)$ *is irreducible over* $\mathbb{F}_p$ *if and only if* p *is of order* $\varphi(N) = N-1$ *modulo* N.

Proof. We get i) since $x^N - 1 = \prod_{d \mid N} \mathcal{Q}_d(x)$ is square free.
ii), iii) and iv) come from Lemma 2.7-ii) with $d = 1$, $d \geq 2$ and $d = N-1$, respectively. □

3. The proof of Theorem 1.1

We refer to Notation 2.4.

3.1. Necessary conditions on the a_j's, Q and b

According to Proposition 2.3, Q and b must satisfy

$$\text{either } p \nmid b+1, \text{ or } b \in \{p-1, 2p-1\},$$

and at least one of the N_j's does not divide $p-1$. In this section, we prove the following proposition.

Proposition 3.1. *If* A *is an even perfect polynomial with* $\omega(A) = p+1$, *then for some* $\xi \in \mathbb{F}_p$,

$$A(x+\xi) = \prod_{j=1}^{p} (x+j)^{N_j p^{n_j}-1} \cdot Q^b,$$

where Q *is irreducible,* $1+Q$ *splits over* $\mathbb{F}_p$, $n_p = n_j = 0$, $N_j \mid p-1$ *for any* $j \neq p$, $b = 1$ *and*
either $N_p = 4$, $Q = 1+x^2$, *or* N_p *is prime,* $N_p \nmid p-1$, $Q = \sigma(x^{N_p-1})$.

We consider the following subsets of $\{1, \ldots, p\}$:

$$\Lambda := \{i : n_i = 0\}, \quad \Sigma_1 := \{i : Q \mid \sigma(P_i^{a_i})\}, \quad \Sigma_2 := \{i : Q \nmid \sigma(P_i^{a_i})\}.$$

Lemma 3.2. *One has* $\Sigma_1 \cap \Sigma_2 = \emptyset$, $\Sigma_1 \cup \Sigma_2 = \{1, \ldots, p\}$ *and* $\Sigma_1 \neq \emptyset$.

Proof. The first two equalities are obviously true. Now, if $\Sigma_1 = \emptyset$, then for any i, $Q \nmid \sigma(P_i^{a_i})$. Since $Q \nmid \sigma(Q^b)$, from Equalities (2.1) in Remark 2.5, we see that Q does not divide A, which is impossible. □

From Lemma 2.2-i), without loss of generality, we may suppose that $p \in \Sigma_1$. Put

$$N := N_p, \quad n := n_p \text{ and } a := a_p = Np^n - 1.$$

3.1.1. First reductions.

Lemma 3.3.
i) *If* $j \in \Lambda \smallsetminus \Sigma_1$, *then* $a_j \leq p-2$.
ii) *If* $j \in \Lambda \smallsetminus \Sigma_1$ *and if* $P_j \mid \sigma({P_k}^{a_k})$, *then* $k \in \Lambda$.

Proof. i) One has

$$a_j = N_j - 1, \quad p \nmid N_j, \quad \sigma({P_j}^{a_j}) = \prod_{l \neq j} {P_l}^{\alpha_{lj}},$$

where $\alpha_{lj} \in \{0,1\}$ by Lemma 2.6.
Thus $a_j = \sum_{l \neq j} \alpha_{lj} \leq p-1$ and $a_j = N_j - 1 \neq p-1$ since $p \nmid N_j$.
ii) If $n_k \geq 1$, then the exponent of P_j in $\sigma({P_k}^{a_k})$ is at least $p^{n_k} - 1$. Hence, from i), $p^{n_k} - 1 \leq a_j \leq p-2$. It is impossible. □

Lemma 3.4.
i) *If* $j \notin \Sigma_1$, *then* $N_j \mid p-1$.
ii) *If* $j-1, j \notin \Sigma_1$ *and if* $n_j \geq 1$, *then* $n_{j-1} \geq 1$.

Proof. Again, we consider equalities (2.1) in Remark 2.5.
i) If $Q \nmid \sigma({P_j}^{a_j})$, then $\sigma({P_j}^{a_j})$ must split over $\mathbb{F}_p$, and thus $N_j \mid p-1$.
ii) If $n_j \geq 1$, then $(P_{j-1})^{p^{n_j}-1} \mid \sigma({P_j}^{a_j})$, and thus $a_{j-1} \geq p^{n_j} - 1 \geq p-1$. Hence, we must have $n_{j-1} \geq 1$, by Lemma 3.3-i). □

Proposition 3.5. *The polynomial* Q *is exactly* $\mathcal{Q}_N(x)$, *and for any proper divisor* l *of* N, *the* l*-th cyclotomic polynomial* $\mathcal{Q}_l(x)$ *splits over* $\mathbb{F}_p$.

Proof. Equalities (2.1) (Remark 2.5) imply that $\sigma({P_p}^{a_p})$ divides A. Moreover, $\sigma({P_p}^{a_p}) = \sigma(x^a) = \sigma(x^{Np^n-1})$ and

$$\sigma(x^{Np^n-1}) = (x-1)^{p^n-1}(1 + x + \cdots + x^{N-1})^{p^n} = (x-1)^{p^n-1}(\sigma(x^{N-1}))^{p^n}.$$

If Q divides $\sigma(x^a)$, then $\sigma(x^{N-1})$ is of the form ${P_1}^{\alpha_1} \dots {P_p}^{\alpha_p} Q^{\alpha}$, where by Lemma 2.6, each $\alpha_j \in \{0,1\}$ and $\alpha = 1$. By Corollary 2.8, we get

$$\prod_{d \mid N,\ d \neq 1} \mathcal{Q}_d(x) = \sigma(x^{N-1}) = {P_1}^{\alpha_1} \cdots {P_p}^{\alpha_p} \cdot Q.$$

If both d and v divide N with $d \neq v$, then $\gcd(\mathcal{Q}_d(x), \mathcal{Q}_v(x)) = 1$ and there exists a unique divisor m of N such that $\mathcal{Q}_m(x) = Q$ and $\mathcal{Q}_l(x)$ splits for any divisor l of N, distinct from m. We claim that $m = N$. If $m \neq N$, then $\mathcal{Q}_N(x)$ splits, so $N \mid p-1$, and thus $x^N - 1$ and $\sigma(x^{N-1})$ split. It is impossible because $Q \mid \sigma(x^{N-1})$. □

Corollary 3.6. *The integer* N *and the prime number* p *satisfy*

$$N = q^u, \quad \text{where } q \text{ is a prime number and } u \in \mathbb{N}^*, \quad p = q^{u-1}v + 1 \text{ with } q \nmid v.$$

Proof. If we write $N = {q_1}^{u_1} \dots {q_r}^{u_r}$ with each q_j prime and $u_j \in \mathbb{N}^*$, and if $r \geq 2$, then for any j, ${q_j}^{u_j} \neq N$. So $\mathcal{Q}_{{q_j}^{u_j}}(x)$ splits, and thus ${q_j}^{u_j}$ divides $p-1$. Hence $N = {q_1}^{u_1} \dots {q_r}^{u_r}$ divides $p-1$, which is impossible. So, $r = 1$ and $N = {q_1}^{u_1}$.

Again, as above, ${q_1}^{u_1-1}$ divides $p-1$, whereas ${q_1}^{u_1} = N$ does not. So $p = {q_1}^{u_1-1} \cdot v + 1$, where $q_1 \nmid v$. □

Corollary 3.7.
i) *If $u = 1$, then $N = q$ is prime, $N \nmid p-1$ and $Q = \sigma(x^{N-1})$.*
ii) *If $u \geq 2$, then $q = 2$, $u = 2$, so that $N = 4$, $Q = \mathcal{Q}_4(x) = 1 + x^2$.*

Proof. i) Proposition 3.5 and Lemma 2.7-i) imply $Q = \mathcal{Q}_N(x) = \sigma(x^{N-1})$ since N is prime.
ii) If q is odd, then $q \geq 3$. Since $p = 1 + q^{u-1}v \equiv 1 \mod q^{u-1}$, one has

$$p^q = (1 + q^{u-1}v)^q = 1 + \sum_{l=1}^{q-1} \binom{q}{l} v^l q^{(u-1)l} + v^q q^{(u-1)q}.$$

But $(u-1)q \geq u$ and for any $1 \leq l \leq q-1$, $q \mid \binom{q}{l}$ and $1 + (u-1)l \geq u$, we get

$$q^u \mid \binom{q}{l} \cdot q^{(u-1)l} \text{ and } q^u \mid q^{(u-1)q}.$$

Thus,

$$p^q \equiv 1 \mod N \text{ and } p^{\frac{\varphi(N)}{2}} \equiv 1 \mod N \text{ since } q \text{ divides } q^{u-1} \cdot \frac{q-1}{2} = \frac{\varphi(N)}{2}.$$

Hence, $\mathcal{Q}_N(x)$ is reducible, which is impossible. So, $q = 2$ and $N = 2^u$.

Now, $p \equiv 1 \mod 2^{u-1}$, and thus $p^2 \equiv 1 \bmod N$. Since $p \not\equiv 1 \mod N$, $\mathcal{Q}_N(x)$ has $\frac{\varphi(N)}{2}$ irreducible divisors of degree 2 and from its irreducibility, one has

$$2^{u-2} = \frac{\varphi(N)}{2} = 1, \quad u = 2 \quad \text{and} \quad p = 2v + 1 \text{ with } v \text{ odd}.$$

Therefore, $N = 4$ and $Q = \mathcal{Q}_4(x) = 1 + x^2$. □

Lemma 3.8. ([**10**, Lemma 4.13]) *Let p be an odd prime number. If $\sigma(x^a)$ is irreducible over $\mathbb{F}_p$ and if $\sigma(x^a) = \sigma((x+\mu)^a)$ for some $\mu \in \mathbb{F}_p$, then $\mu = 0$.*

Corollary 3.9.
i) *One has: $\#\Sigma_1 = 1$ and $b = p^{n_l}$ if $\Sigma_1 = \{l\}$.*
ii) *The polynomial $1 + Q$ must split over $\mathbb{F}_p$.*

Proof. i) If $\#\Sigma_1 \geq 2$, then we may suppose that $\{j, p\} \subset \Sigma_1$ for some $j \neq p$. Hence, by Corollary 3.7 and by Lemma 3.8

$$Q \in \{1 + x^2, \sigma(x^{N-1})\} \cap \{1 + (x+j)^2, \sigma((x+j)^{N_j-1})\} = \emptyset, \text{ which is impossible.}$$

So, we may put $\Sigma_1 = \{l\}$. One has

$$Q^{p^{n_l}} \parallel \sigma((x+l)^{a_l}),\ Q^{p^{n_l}} \parallel \sigma(A) = A, \quad \text{and} \quad b = p^{n_l}.$$

ii) b is odd by i), so $1+Q$ divides $\sigma(Q^b)$, and hence it divides $\sigma(A) = A$. Therefore, $1 + Q$ must split over $\mathbb{F}_p$. □

3.1.2. Consequences of the splitting condition on $1+Q$. We have just seen that $1+Q$ must split over $\mathbb{F}_p$. If $N=4$ so that $Q=1+x^2$, then (-2) is a square in $\mathbb{F}_p$. If N is an odd prime number, then

$$1+Q=1+\sigma(x^{N-1})=\frac{x^N+x-2}{x-1}.$$

So, $1+Q$ splits if and only if x^N+x-2 splits.

In this section, we give some properties obtained from the splitting condition over $\mathbb{F}_p$ on the polynomial x^N+x-2, where N is an odd prime number.

Put

$$S:=x^N+x-2$$

and suppose that S splits (here, S may not be square free)

$$S=(x-\xi_1)\dots(x-\xi_N),\ \text{where each } \xi_j\in\mathbb{F}_p\smallsetminus\{0\}\ \text{ and }\ \xi_1=1.$$

Consider the elementary symmetric polynomials of these N roots of S

$$\begin{aligned} s_1&:=\sum_{j=1}^{N}\xi_j, & s_2&:=\sum_{1\le j<k\le N}\xi_j\cdot\xi_k,\dots,\\ s_N&:=\xi_1\cdots\xi_N, & s_m&:=0\quad\text{if }\ m>N, \end{aligned}$$

and Newton's Formula (see, e.g., [**13**])

$$T_m:=\sum_{j=1}^{N}(\xi_j)^m=\sum_{j=1}^{m-1}(-1)^{j-1}\cdot s_j\cdot T_{m-j}+(-1)^{m-1}\cdot m\cdot s_m\qquad\text{for } m\in\mathbb{N}.$$

Lemma 3.10. *One has*

$$\begin{aligned} T_0&=N, & T_j&=0\ \ \textit{if } 1\le j\le N-2,\\ T_{N-1}&=-(N-1)s_{N-1}=-N+1, & T_{N+j}&=-T_{j+1}+2T_j\ \ \textit{for any } j\in\mathbb{N}. \end{aligned}$$

In particular,

$$\begin{aligned} T_N&=2N, & T_j&=0\ \ \textit{if } N+1\le j\le 2N-3,\\ T_{2N-2}&=N-1, & T_{2N-1}&=-4N+2,\\ T_{2N}&=4N, & T_{p-1}&=-T_{p-N}+2T_{p-1-N}. \end{aligned}$$

Proof. We get

$$x^N+x-2=x^N-s_1x^{N-1}+\cdots+(-1)^{N-1}s_{N-1}\,x+(-1)^Ns_N,$$

and since N is odd

$$s_1=\cdots=s_{N-2}=0,\quad s_{N-1}=1,\quad s_N=2,\quad s_m=0\ \text{ if } m\ge N+1.$$

Therefore, Newton's formula gives

$$\begin{aligned} T_0&=N, & T_j&=0 \text{ if } 1\le j\le N-2,\\ T_{N-1}&=-(N-1)s_{N-1}=-N+1, & T_{N+j}&=-T_{j+1}+2T_j \text{ for any } j\in\mathbb{N}. \end{aligned}$$

Thus

$$\begin{aligned} T_N &= 2N, \\ T_{N+j} &= 0 \text{ if } 1 \le j \le N-3, \\ T_{2N-2} &= -T_{N-1} + 2T_{N-2} = -(-N+1) + 0 = N-1, \\ T_{2N-1} &= -2N + 2(-N+1) = -4N + 2, \\ T_{2N} &= -0 + 2(2N) = 4N, \\ T_{2N+1} &= -T_{N+2} + 2 \cdot 0 = -T_{N+2}, \\ T_{p-1} &= T_{N+p-N-1} = -T_{p-N} + 2T_{p-1-N}. \end{aligned}$$

□

Corollary 3.11. *If N is an odd prime number such that $N \nmid p-1$ and if $S = x^N + x - 2$ splits over $\mathbb{F}_p$, then*

$$N = 3 \text{ and } (-7) \text{ is a square in } \mathbb{F}_p, \qquad \text{or} \qquad 5 \le N \le \frac{p-3}{2} \le p-2.$$

In particular, $p \ge 2N+3$.

Proof.

- If $N = 3$, then $S = x^3 + x - 2 = (x-1)(x^2+x+2)$ and the discriminant of x^2+x+2 is -7. So, (-7) must be a square in $\mathbb{F}_p$. Therefore, $p \equiv 1, 2, 4 \mod 7$ (use Legendre symbol). So, $p \ge 11 \ge 2 \cdot 3 + 3$.
- Now, we suppose that $N \ge 5$. We remark that

$$T_{p-1} = \sum_{j=1}^{N} (\xi_j)^{p-1} = \sum_{j=1}^{N} 1 = N.$$

Since both p and N are odd (and prime), we must have

$$p \notin \{N-1, N+1\}, \text{ and thus } (p \le N-2) \text{ or } (p \ge N+2).$$

From Lemma 3.10, we get the following contradictions (modulo p):
– If $p \le N-2$, then $p-1 \le N-3$, so $0 = T_{p-1} = N$.
– If $N+2 \le p \le 2N-2$, then $1 \le p-1-N \le p-N \le N-2$, so

$$0 = -T_{p-N} + 2T_{p-N-1} = T_{p-1} = N.$$

– If $p = 2N-1$, then $N-1 = T_{2N-2} = T_{p-1} = N$.
– If $p = 2N+1$, then $4N = T_{2N} = T_{p-1} = N$ with $N \ge 5,\ p \ge 11$.
We conclude that $p \ge 2N+3$.

□

Corollary 3.12. *One has $\#\Lambda \in \{0, p\}$.*

Proof. By Corollary 3.9 and Lemma 2.2-i) and suppose without loss of generality, we may that $\Sigma_1 = \{p\}$.

– If $n_{p-1} \ge 1$, then by Lemma 3.4, one has $n_{p-2} \ge 1$. Again by the same lemma, we get $n_{p-3} \ge 1$ and so on $n_{p-4}, \ldots, n_1 \ge 1$.
Since $N_p = N \le p-2$ by Corollary 3.11 and since $x^{p^{n_1}-1} \| \sigma({P_1}^{a_1})$, we get

$$N \cdot p^{n_p} - 1 = a_p \ge p^{n_1} - 1 \ge p - 1, \quad \text{and thus} \quad n_p \ge 1.$$

So, $n_j \ge 1$ for any j, and $\Lambda = \emptyset$.

– If $n_{p-1} = 0$, since $p-1 \notin \Sigma_1$, we get

$$p-2 \geq N_{p-1} - 1 \geq p^{n_p} - 1, \quad \text{and thus} \quad n = n_p = 0.$$

By the same argument, one has $n_1 = 0, \ldots, n_{p-2} = 0$.
So for any j, $n_j = 0$ and $\#\Lambda = p$.

□

Lemma 3.13. *Let U be an irreducible polynomial over $\mathbb{F}_p$ and $v \in \mathbb{N}$. Then*

i) $\gcd(1+U, 1+(U^2)^1 + \cdots + (U^2)^{\frac{p^v-1}{2}}) = 1$.

ii) *If $\sigma(U^{p^v})$ splits over $\mathbb{F}_p$, then $v = 0$.*

Proof. i) If T is a common irreducible divisor of $1+U$ and $1+(U^2)^1 + \cdots + (U^2)^{\frac{p^v-1}{2}}$, then one has modulo T

$$U \equiv -1, \qquad U^2 \equiv 1 \qquad \text{and} \qquad \frac{p^v+1}{2} \equiv 1 + (U^2)^1 + \cdots + (U^2)^{\frac{p^v-1}{2}} \equiv 0.$$

Thus $\dfrac{p^v+1}{2} \equiv 0 \mod p$, which is impossible since p does not divide p^v+1.
ii) Put

$$\frac{U^{p^v+1}-1}{U-1} = \sigma(U^{p^v}) = \prod_j (x-\xi_j)^{\alpha_j},$$

where each ξ_j lies on $\mathbb{F}_p$ and $\alpha_j \in \mathbb{N}^*$.
If $v \geq 1$, then one has

$$\prod_j (x-\xi_j)^{\alpha_j} = \sigma(U^{p^v}) = (1+U) \cdot \Big(1 + (U^2)^1 + \cdots + (U^2)^{\frac{p^v-1}{2}}\Big),$$

where $\gcd\Big(1+U, 1+(U^2)^1 + \cdots + (U^2)^{\frac{p^v-1}{2}}\Big) = 1$ by i).
We obviously remark that $U(\xi_j) \neq 1$ for any j. So

$$U(\xi_j) + 1 = \frac{(U(\xi_j))^2 - 1}{U(\xi_j) - 1} = \frac{(U(\xi_j))^{p^v} \cdot U(\xi_j) - 1}{U(\xi_j) - 1} = (\sigma(U^{p^v}))(\xi_j) = 0.$$

Thus $\prod_j (x-\xi_j)$ divides $1+U$. It follows that $1 + (U^2)^1 + \cdots + (U^2)^{\frac{p^v-1}{2}} = 1$, which is impossible because $v \geq 1$. □

Corollary 3.14. *If $A = {P_1}^{a_1} \cdots {P_p}^{a_p} \cdot Q^b$ is perfect, then $b = 1$ and for any $j \in \{1, \ldots, p\}$,*

$$n_j = 0, \ a_j = N_j - 1 \leq p-2, \qquad \textit{where} \ \ N_j \mid p-1 \ \textit{if} \ j \notin \Sigma_1.$$

Proof. We also need Corollary 3.9 and Lemma 2.2-i) in order to suppose that $\Sigma_1 = \{p\}$. We apply Lemma 3.13 with $U = Q$ and $v = n_p$. We get

$$n_p = 0 \quad \text{and} \quad b = p^{n_p} = 1.$$

Therefore, $\Lambda \neq \emptyset$, and thus $\Lambda = \{1, \ldots, p\}$ by Corollary 3.12.
We know that $N_p \leq p-2$ and for any $j \neq p$, $N_j \mid p-1$ by Lemma 3.4-i), since $j \notin \Sigma_1$. □

We obtain Proposition 3.1 from Proposition 3.5, Corollaries 3.7, 3.9 and 3.14.

3.2. More precisions about the N_j's

We recall that for some $\xi \in \mathbb{F}_p$, $A(x+\xi) = \prod_{j=1}^{p}(x+j)^{N_j-1} \cdot Q$, $N_j \mid p-1$ if $j \neq p$ and either ($N_p = 4, Q = 1+x^2$) or (N_p odd prime, $Q = \sigma(x^{N_p-1})$).
We would like to give more details about the N_j's. We are mainly inspired by the proof of [**2**, Theorem 1].
Put

$$B := \prod_{j=1}^{p}(x+j)^{N_j-1} \qquad \text{and} \qquad m := \min\{N_j : 1 \leq j \leq p\}.$$

First, by Lemma 2.2-ii), one has $m \geq 2$. We prove that $\#\{j : N_j = m\} = 1$ and $m \in \{2, N_p - 1, N_p\}$ which corresponds to the conditions (1), (2) and (3), respectively, described in Theorem 1.1.

For $l, \lambda \in \mathbb{N}$ such that $l \leq \deg(B)$, $\lambda \mid p-1$ and $2 \leq \lambda \leq m$, $B^{(l)}$ denotes the sum of all distinct monic divisors of B degree $\deg(B) - l$, where $\tau B^{(l)}$ is the number of distinct summands of $B^{(l)}$ and $B_\lambda := (x^p - x)^{\lambda-1}$. We get next lemmas.

Lemma 3.15. *Any polynomial of degree at most equal to $\lambda - 1$ divides B if and only if it divides B_λ.*

Proof. We may write $B = B_\lambda \cdot \prod_{N_j > \lambda}(x+j)^{N_j-\lambda}$.
We obviously get $D \mid B_\lambda \Rightarrow D \mid B$.
Now, if $D \mid B$ with $\deg(D) \leq \lambda - 1$, then $D = x^{l_0} \dots (x+p-1)^{l_{p-1}}$, where $l_0 + \cdots + l_{p-1} \leq \lambda - 1$. So, for any j, $0 \leq l_j \leq \lambda - 1$, D divides $x^{\lambda-1} \dots (x+p-1)^{\lambda-1} = B_\lambda$. □

Lemma 3.16.
i) *The polynomial B_λ is perfect over $\mathbb{F}_p$,*
ii) $\tau B_\lambda^{(\lambda)} \equiv 0 \mod p$,
iii) $\tau B^{(\lambda)} \equiv -k \mod p$, *where* $k := \#\{j : N_j = \lambda\} \leq p$.

Proof. i) It immediately follows from [**1**, Theorem 4].

ii) Every summand of $B_\lambda^{(\lambda)}$ is of the form $\frac{B_\lambda}{x^{l_0} \cdots (x+p-1)^{l_{p-1}}}$, where $l_0 + \cdots + l_{p-1} = \lambda$ and $0 \leq l_j \leq \lambda - 1$.
So, the counting gives (see [**3**, p. 23]) $\tau B_\lambda^{(\lambda)} = \frac{p(p+1)\cdots(p+\lambda-1)}{\lambda!} - p$, which is congruent to 0 modulo p since $\lambda \leq p-1$.

iii) Let C be a summand of $B^{(\lambda)}$. Then $C \in \Gamma_1 \cup \Gamma_2$, where

$$\Gamma_1 = \left\{ \frac{B}{x^{l_0} \cdots (x+p-1)^{l_{p-1}}} : \sum_{i=0}^{p-1} l_i = \lambda,\ l_i \leq \lambda - 1 \right\},$$

$$\Gamma_2 = \left\{ \frac{B}{(x+j)^\lambda} : N_j > \lambda \right\}.$$

If $C \in \Gamma_1$, then B divides CB_λ and $\dfrac{CB_\lambda}{B}$ is a summand of $B_\lambda^{(\lambda)}$.
Conversely, any summand of $B_\lambda^{(\lambda)}$ may be written as $\dfrac{CB_\lambda}{B}$ with $C \in \Gamma_1$.
It follows that

$$\#\Gamma_1 = \tau B_\lambda^{(\lambda)} \quad \text{and} \quad \tau B^{(\lambda)} = \#(\Gamma_1 \cup \Gamma_2) = \#\Gamma_1 \ + \ \#\Gamma_2 = \tau B_\lambda^{(\lambda)} + (p-k).$$

Thus, from ii) $\tau B^{(\lambda)} \equiv -k \mod p$. □

Proposition 3.17. *One has $\#\{j : N_j = m\} = 1$. Moreover,*
- *if $m \neq N_p$, then $m \mid p-1$ and $m = \deg(Q) \in \{2, N_p - 1\}$,*
- *if $m = N_p$, then N_p is a prime number and $N_p \geq 5$.*

Proof. The proof is also inspired by that of Theorem 1 in [**2**]. One has

$$A = B \cdot Q = (x^p - x)^{m-1} \cdot \prod_{N_j > m} (x+j)^{N_j - m} \cdot Q = B_m \cdot \prod_{N_j > m} (x+j)^{N_j - m} \cdot Q.$$

• If $m \neq N_p$, then m divides $p-1$ because $N_j \mid p-1$ whenever $j \neq p$. We apply Lemmas 3.15 and 3.16 with $\lambda = m$. So,

B_m is perfect over $\mathbb{F}_p$ and $\tau B_m^{(m)} \equiv 0 \mod p$ (Lemma 3.16, parts i) and ii)).

If D is a polynomial with $\deg(D) \leq m-1$, then by Lemma 3.15, $D \mid B$ if and only if $D \mid B_m$. Therefore, for any $1 \leq l \leq m-1$,

$$B^{(l)} = \sum_{\substack{\deg(D)=l \\ D \mid B}} \frac{B}{D} = \frac{B}{B_m} \cdot B_m^{(l)}.$$

The fact: $\tau B_m^{(m)} \equiv 0 \mod p$ implies that $\deg(B_m^{(m)}) < \deg(B_m) - m$. So,

$$\deg\left(\sum_{l=m}^{(m-1)p} B_m^{(l)}\right) = \deg\left(B_m^{(m)} + \sum_{l=m+1}^{(m-1)p} B_m^{(l)}\right) < \deg(B_m) - m.$$

From the perfectness of B_m we get $\sum_{l=1}^{(m-1)p} B_m^{(l)} = \sigma(B_m) - B_m = 0$. Therefore,

$$\sum_{l=1}^{m-1} B^{(l)} = \frac{B}{B_m} \cdot \sum_{l=1}^{m-1} B_m^{(l)} - \frac{B}{B_m} \cdot \sum_{l=1}^{(m-1)p} B_m^{(l)} = -\frac{B}{B_m} \cdot \sum_{l=m}^{(m-1)p} B_m^{(l)},$$

$$\deg\left(\sum_{l=1}^{m-1} B^{(l)}\right) = \deg(B) - \deg(B_m) + \deg\left(\sum_{l=m}^{(m-1)p} B_m^{(l)}\right) < \deg(B) - m.$$

Put

$$k := \#\{j : N_j = m\}.$$

We have
$k \geq 1$, $k \leq p-1$ since $m \neq N_p$ and by Lemma 3.16-iii), $\tau B^{(m)} \equiv -k \mod p$.
Thus $\tau B^{(m)} \not\equiv 0 \mod p$.
We claim that $\tau B^{(m)} \equiv -1 \mod p$. Since $\sigma(Q) = 1 + Q$, we get

$$\sigma(A) = \sigma(B) \cdot \sigma(Q) = (B + B^{(m)} + V) \cdot (1 + Q),$$

where $V = \sum_{l=1}^{m-1} B^{(l)} + \sum_{l=m+1}^{\deg(B)} B^{(l)}$, $\deg(V) < \deg(B) - m$.
Hence

$$W := B + (1+Q)(B^{(m)} + V) = (B + B^{(m)} + V) \cdot (1+Q) - BQ$$
$$= \sigma(A) - A = 0.$$

Since $\tau B^{(m)} \not\equiv 0 \mod p$, we have

$$\deg(B) = \deg((1+Q)(B^{(m)} + V)) = \deg(Q) + \deg(B) - m.$$

Hence $m = \deg(Q)$.

From the nullity of W, we deduce that the coefficient of $x^{\deg(B)}$ in W must be equal to 0, that is $1 + \tau B^{(m)} \equiv 0 \mod p$. So, $\tau B^{(m)} \equiv -1 \mod p$.

We have just seen that $m = \deg(Q)$. It remains to show that $m \in \{2, N_p - 1\}$:
– If $N_p = 4$, then $Q = 1 + x^2$ so that $m = \deg(Q) = 2$.
– If N_p is a prime number, then $Q = \sigma(x^{N_p - 1})$ and $m = \deg(Q) = N_p - 1$.

Finally, we have $k = 1$ because $-k \equiv \tau B^{(m)} \equiv -1 \mod p$ and $1 \leq k \leq p - 1$.

• If $m = N_p$, then m does not divide $p - 1$, and thus $m \geq 3$. Since N_j divides $p - 1$ for any $j \neq p$, one has $\#\{j : N_j = m\} = \#\{p\} = 1$.

Let v be the greatest integer such that $v \mid p - 1$ and $v < m$. One has $v \geq 2$. We apply Lemmas 3.15 and 3.16 with $\lambda = v$. So, B_v is perfect over $\mathbb{F}_p$, $\tau B_v^{(v)} \equiv 0 \mod p$, and $\tau B^{(v)} \equiv -k \mod p$, where $k = \#\{j : N_j = v\}$.

Since $k = 0$, we get $\tau B^{(v)} \equiv 0 \mod p$ and $\deg(B^{(v)}) < \deg(B) - v$. Therefore,

$$G := B + (1+Q)(B^{(v)} + E) = (B + B^{(v)} + E) \cdot (1+Q) - BQ$$
$$= \sigma(A) - A = 0,$$

where $E = \sum_{l=1}^{v-1} B^{(l)} + \sum_{l=v+1}^{\deg(B)} B^{(l)}$, $\deg(E) < \deg(B) - v$.

Since $G = 0$, we have

$$\deg(B) = \deg(Q) + \deg(B^{(v)} + E) < \deg(Q) + \deg(B) - v.$$

It follows that $\deg(Q) \geq v + 1 \geq 3$.

Hence, by Corollary 3.7, $N_p \neq 4$ and N_p is a prime number.
Thus $N_p - 1 = \deg(\sigma(x^{N_p - 1})) = \deg(Q) \geq 3$ and $N_p \geq 5$, N_p being prime. □

Corollary 3.18. *One has* $\#\{j : 1 \leq j \leq p, N_j = 2\} \leq 1$.

Proof. From Proposition 3.17, $m \in \{2, N_p, N_p - 1\}$ and $\#\{j : N_j = m\} = 1$. Thus, $m \geq 2$ and we are done. □

3.2.1. Case $N_p = 4$**.** Proposition 3.17 implies that there exists a unique $j_1 \neq p$ such that $N_{j_1} = 2 < N_j$ for any $j \neq j_1$. So, we get the condition (1) of Theorem 1.1. Lemma 3.19 below (obtained by considering the Legendre symbol $\left(\frac{-}{p}\right)$) gives the necessary condition on the prime p.

Lemma 3.19. *Let p be an odd prime number. The polynomial $1 + x^2$ is irreducible over $\mathbb{F}_p$ and $2 + x^2$ splits over $\mathbb{F}_p$ if and only if ((-1) is not a square in $\mathbb{F}_p$ and (-2) is a square) if and only if $p \equiv 3 \mod 8$.*

3.2.2. Case where N_p is an odd prime such that $N_p \nmid p-1$. From Corollaries 3.14 and 3.11, we recall that

$$\sigma(x^{a_p}) = \sigma(x^{N_p-1}) = Q, \qquad \sigma(Q) = 1+Q \text{ splits over } \mathbb{F}_p, \text{ and } p \geq 2N_p+3.$$

Lemma 3.20. *If there exists $j_1 \neq p$ such that $N_{j_1} = N_p - 1$, then j_1 is unique and $N_j > N_{j_1}$ for any $j \neq j_1$.*

Proof. Since N_p is a prime number, we get $N_p - 1 = \deg(\sigma(x^{N_p-1})) = \deg(Q)$. Thus, Proposition 3.17 implies that

$$1 = \#\{j \in \mathbb{F}_p : N_j = m\} = \#\{j \in \mathbb{F}_p : N_j = \deg(Q) = N_p - 1\}.$$

□

We get more precisions when $N_p = 3$:

♢ $Q = 1 + x + x^2$ is irreducible,

♢ $\sigma(Q) = 2 + x + x^2$ splits over $\mathbb{F}_p$, so that the discriminant of Q, -3, is not a square in $\mathbb{F}_p$ and -7 is a square.

Again, by using the Legendre symbol, we obtain that p must satisfy: $p \equiv 2, 8$ or 11 mod 21.

4. Proof of Corollary 1.4

In this section, from Lemma 4.1, we prove that if the N_j's lie on some special set of divisors of $p-1$ (in particular, if p is a safe prime), then there does not exist any even perfect polynomial A over $\mathbb{F}_p$ with $p+1$ irreducible factors.

Lemma 4.1. *For any $u \in \mathbb{F}_p$, one has*

$$\#\{j \in \mathbb{F}_p : (j-u) \neq 1,\ (j-u)^{N_j} = 1\} = N_u - 1 \quad \text{if } x+u \nmid \sigma(Q),$$
$$\#\{j \in \mathbb{F}_p : (j-u) \neq 1,\ (j-u)^{N_j} = 1\} = N_u - 2 \quad \text{if } x+u \mid \sigma(Q).$$

In particular, $\#\{j \in \mathbb{F}_p : j \neq 1,\ j^{N_j} = 1\} = N_p - 1$.

Proof. It suffices to remark that for a fixed $u \in \mathbb{F}_p$, $x+u$ divides $\sigma((x+j)^{a_j})$ if and only if $(j-u)^{N_j} = 1$ and $(j-u) \neq 1$. Compare then the exponents of $x+u$ in A and in $\sigma(A)$. □

Corollary 4.2.

i) *If for any $j \neq p$, $N_j \in \{2, \frac{p-1}{2}, p-1\}$, then A is not perfect.*

ii) *If p is a safe prime, then there exist no such perfect polynomials over $\mathbb{F}_p$.*

Proof. Put $H := \{j \in \mathbb{F}_p :\ j \neq 1,\ j^{N_j} = 1\}$ and ${\mathbb{F}_p}^2 := \{t^2 : t \in \mathbb{F}_p\}$. We have $\#H = N_p - 1$ by Lemma 4.1, and

$$\{j \in \mathbb{F}_p : j^{N_j} \neq 1\} \subset \{j \in \mathbb{F}_p : N_j = 2\} \cup \left\{ j \notin {\mathbb{F}_p}^2 : N_j = \frac{p-1}{2} \right\}.$$

So $\mathbb{F}_p \smallsetminus H$ is contained in $\{1\} \cup \{j \in \mathbb{F}_p : N_j = 2\} \cup (\mathbb{F}_p \smallsetminus {\mathbb{F}_p}^2)$, and

$$p - (N_p - 1) = \#(\mathbb{F}_p \smallsetminus H) \leq 1 + 1 + \frac{p-1}{2}, \text{ by Corollary 3.18.}$$

Hence, $p \leq 2N_p + 1$, which contradicts Corollary 3.11. □

References

1. Beard J. T. B. Jr, O'Connell J. R. Jr, West K. I., *Perfect polynomials over $GF(q)$* Rend. Accad. Lincei, **62** (1977), 283–291.

2. Beard J. T. B. Jr., *Perfect polynomials revisited* Publ. Math. Debrecen, **38(1-2)** (1991), 5–12.

3. Berge C., *Principles of Combinatorics*, New York 1971.

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

5. Dickson L. E., *Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors* American J. ???, **35** (1913), 413–422.

6. Dubner H., *Large Sophie Germain primes*, Math. Comp., **65** (1996), 393–396.

7. Gallardo L., Rahavandrainy O., *Perfect polynomials over $\mathbb{F}_4$ with less than five prime factors*, Port. Math., **64(1)** (2007), 21–38.

8. Gallardo L., Rahavandrainy O., *Odd perfect polynomials over $\mathbb{F}_2$*, J. Théor. Nombres Bordeaux, **19** (2007), 167–176.

9. Gallardo L., Rahavandrainy O., *On perfect polynomials over $\mathbb{F}_p$ with p irreducible factors*, Port. Math., **69(4)** (2012), 283–303.

10. Gallardo L., Rahavandrainy O., *Perfect polynomials over $\mathbb{F}_p$ with $p+1$ irreducible divisors*, Acta Math. Univ. Comenian. (N.S.), **LXXXIII(1)** (2014), 93–112.

11. Indlekofer K. H., Járai A., *Largest known twin primes and Sophie Germain primes* Math. Comp., **68** (1999), 1317–1324.

12. Lidl R., Niederreiter H., *Finite Fields, Encyclopedia of Mathematics and its applications*, Cambridge University Press, 1983, (Reprinted 1987).

13. Mead D. G., *Newton's Identities* Amer. Math. Monthly **99(8)** (1992), 749–751.

14. Nyblom M. A., *Sophie Germain primes and the exceptional values of the equal-sum-and-product problem*, Fibonacci Quart. **50(1)** (2012), 58–61.

15. OEIS, *On-line Encyclopedia of Integer Sequences*, `https://oeis.org`.

16. Serre J.-P., *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.), **40(4)** (2003), 429–440.

17. Yates S., *Sophie Germain primes, The mathematical heritage of C. F. Gauss*, World Sci. Publ., River Edge, NJ, (1991), 882–886.

L. H. Gallardo, Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France, *e-mail*: `Luis.Gallardo@univ-brest.fr`

O. Rahavandrainy, Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France, *e-mail*: `Olivier.Rahavandrainy@univ-brest.fr`