ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 41, Number 3, 2011

ON KRONECKER POLYNOMIALS

AHMED AYACHE, OTHMAN ECHI AND MONGI NAIMI

ABSTRACT. Monic polynomials with integer coefficients having all their roots in the unit disc have been studied by Kronecker; they are called *Kronecker polynomials*. Let $n \geq 1$ be an integer. By a *strong Kronecker polynomial*, we mean a monic polynomial $P(X) \in \mathbf{Z}[X]$ of degree $n-1$ and such that $P(X)$ divides $P(X^t)$ for each $t \in \{1, \dots, n-1\}$. We say that $P(X)$ is an *absolutely Kronecker polynomial* if $P(X)$ divides $P(X^t)$ for each positive integer t. We describe a canonical form of strong (respectively absolute) Kronecker polynomials. We, also, prove that if n is composite, then each strong Kronecker polynomial with degree $n-1$ is absolutely Kronecker. If n is prime, then we prove that each strong Kronecker polynomial $P(X) \neq 1 + X + X^2 + \dots + X^{n-1}$ is absolutely Kronecker.

0. Introduction. In 1857, Kronecker [**4**] was interested in monic polynomials (i.e., with highest coefficient 1) with integer coefficients having all their roots in the unit disc (Kronecker polynomials). Kronecker proved that the non-zero roots of such polynomials are on the boundary of the unit disc (the unit circle); he also proved that there are finitely many such polynomials of degree a given positive integer n.

In 2001, Pantelis Damianou [**3**] described a canonical form of these polynomials and called them *Kronecker polynomials*. He proved that these polynomials have the form $P(X) = X^k Q(X)$, where $Q(X)$ is a finite product of cyclotomic polynomials.

In 2000, Doru Caragea and Viviana Ene proposed the following "Millennial polynomial problem" [**1**]: Let S be the set of monic, irreducible polynomials with degree 2000 and integer coefficients. Find all $P \in S$ such that $P(a)$ divides $P(a^2)$ for every natural number a.

2010 AMS *Mathematics subject classification.* Primary 11A41, 11A51, 11C08, 12D05.
Keywords and phrases. Euler totient function, cyclotomic polynomial, prime number, reciprocal polynomial, zeros on the unit circle.
The second author is the corresponding author.
Received by the editors on June 17, 2008, and in revised form on October 3, 2008.

DOI:10.1216/RMJ-2011-41-3-707

The above problem has been solved in [**2**]. The authors have described all monic polynomials $P(X)$ with integer coefficients such that $P(X)$ divides $P(X^2)$; as $P(X) = X^{k_0} \prod_{n=1}^{\infty} \phi_i(X)^{k_n}$, where ϕ_i is the ith cyclotomic polynomial, $k_n = 0$ for all but finitely many n and $k_n \geq k_{2n}$, for all n.

We introduce the following polynomial concepts.

Definitions 0.1. Let $P(X)$ be a monic polynomial in $\mathbf{Z}[X]$.

(1) We say that $P(X)$ is a *strong Kronecker polynomial* (SK-*polynomial, for short*) if $P(X)$ divides $P(X^t)$ for each $t \in \{1, \ldots, n-1\}$, where $n = 1 + \deg(P)$. The set of SK-polynomials with degree $n-1$ will be denoted by $SK[n]$.

(2) $P(X)$ is said to be an *absolutely Kronecker polynomial* (AK-*polynomial, for short*) if $P(X)$ divides $P(X^t)$ for each $t \in \mathbf{N} \setminus \{0\}$. The set of all AK-polynomials of degree $n-1$ will be denoted by $AK[n]$.

The justification for calling these polynomials Kronecker will become clear later.

Since the set of Kronecker polynomials of degree a given natural number n is finite [**4**], the sets $SK[n]$ and $AK[n]$ are, also, finite.

Now, we are in a position to state the following problem.

Problem 0.2. For a given integer $n \geq 2$, determine explicitly the sets, $SK[n]$ and $AK[n]$.

In what follows, we denote by $A_n(X)$ the polynomial

$$A_n(X) := 1 + X + X^2 + \ldots + X^{n-1}.$$

We prove, here, that $AK[n] = SK[n] \setminus \{A_n(X)\}$ if and only if n is prime and a positive integer $n \geq 2$ satisfies $AK[n] = SK[n]$ if and only if n is a composite number.

Let $\phi_i(X)$ be the ith cyclotomic polynomial and $\varphi(i)$ the value of the Euler totient on i. Our main result is Theorem 3.9 which states that for an integer $k \geq 2$, a monic polynomial $P(X)$ of degree $k-1$ which does not vanish on 0 is an AK-polynomial if and only if there exist integers $\alpha_1, \alpha_2, \dots, \alpha_{k-1} \geq 0$ such that $P(X) = \prod_{i=1}^{k-1}(\phi_i(X))^{\alpha_i}$, with the property that $k-1 = \sum_{i=1}^{k-1} \alpha_i \varphi(i)$; and $\alpha_i \geq \alpha_j$ whenever i divides j.

1. Prime numbers.

One of the aims of this paper is to link arithmetical properties in $\mathbf{Z}$ with polynomial properties in the ring $\mathbf{Z}[X]$.

For an integer $k \geq 2$, consider the polynomial $A_k(X) := 1 + X + \cdots + X^{k-1}$. Then, we prove that k is prime if and only if for each natural number n a non multiple of k, the polynomial $A_k(X)$ divides $A_k(X^n)$ in the ring $\mathbf{Z}[X]$ (cf., Theorem 1.3).

We, also, prove that n, k are relatively prime if and only if the polynomial $A_k(X)$ divides $A_k(X^n)$ in the ring $\mathbf{Z}[X]$(cf., Proposition 1.4).

In [**5**], Nieto has discussed the divisibility of polynomials with integer coefficients. Let $f \in \mathbf{Z}[X]$. Then we denote by $c(f)$ the content of f (i.e., the greatest common divisor of its coefficients).

Let us recall Nieto's results.

Theorem 1.1. *Let $f, g \in \mathbf{Z}[X]$. Then g divides f in $\mathbf{Z}[X]$ if and only if $c(g)$ divides $c(f)$ and $g(n)$ divides $f(n)$ for infinitely many $n \in \mathbf{Z}$.*

As an application of Theorem 1.1, Nieto has proved the following.

Theorem 1.2. *Let $k \geq 2$ be a fixed integer. Then the non constant irreducible monic polynomials $f \in \mathbf{Z}[X]$ such that $f(n)$ divides $f(n^k)$ for all integers n are the cyclotomic polynomials with order j coprime with k.*

Direct application of Nieto's results yields the following.

Theorem 1.3. *Let $k \geq 2$ be an integer, and let $P(X)$ be one of the two polynomials $\phi_k(X)$ or $A_k(X) := 1 + X + \cdots + X^{k-1}$. Then the following statements are equivalent*:

(i) *k is prime*;

(ii) *for each natural number n non multiple of k, the polynomial $P(X)$ divides $P(X^n)$ in the ring $\mathbf{Z}[X]$.*

Proof. (i) $\Rightarrow$ (ii). If k is prime, then $P(X) = \phi_k(X)$; and the result follows trivially by combining Theorems 1.1 and 1.2.

(ii) $\Rightarrow$ (i). Suppose that k is not prime. Then there exist two integers $p, q \geq 2$ such that $k = pq$.

(a) Suppose that $P(X) = \phi_k(X)$. Let λ be a kth primitive root of unity. Then λ^p is a root of $\phi_k(X)$ (since $P(X)$ divides $P(X^p)$). But, as $\gcd(k, p) \neq 1$, λ^p is not a kth primitive root of unity, contradicting the definition of $\phi_k(X)$.

(b) Suppose that $P(X) = A_k(X)$. Let $\mu := \exp(2i\pi/k)$. Then μ^q is a root of A_k. Since, in addition, $P(X)$ divides $P(X^p)$, $(\mu^q)^p$ is a root of A_k. This leads to $A_k(1) = 0$; a contradiction.

Therefore, k is a prime number. □

The following proposition translates the notion of relatively prime numbers into a division in the ring $\mathbf{Z}[X]$.

Proposition 1.4. *Let $n, k \in \mathbf{N} \setminus \{0, 1\}$ and $P(X)$ be one of the two polynomials $\phi_k(X)$ or $A_k(X)$. Then the following statements are equivalent*:

(i) *n, k are relatively prime*;

(ii) *the polynomial $P(X)$ divides $P(X^n)$ in the ring $\mathbf{Z}[X]$.*

Proof. (i) $\Rightarrow$ (ii). If we suppose that $P(X) = \phi_k(X)$, then the implication follows immediately from Nieto's results (Theorems 1.1 and 1.2).

Now, suppose that $P(X) = A_k(X)$. Let us denote by $\lambda := \exp(2i\pi/k)$; then $A_k(X) = (X - \lambda)(X - \lambda^2) \cdots (X - \lambda^{k-1})$.

To prove that $A_k(X)$ divides $A_k(X^n)$, it is sufficient to show that $\lambda^{tn} \neq 1$, for each $t \in \{1, \dots, k-1\}$. Indeed, since $\gcd(n, k) = 1$, n is invertible modulo k; and consequently, $tn \not\equiv 0 \pmod{k}$, for each $t \in \{1, \dots, k-1\}$. Thus, $\lambda^{tn} \neq 1$.

(ii) $\Rightarrow$ (i). The hypothesis implies that $nt \not\equiv 0 \pmod{k}$, for each $t \in \{1, \dots, k-1\}$. Hence the map $\psi : \mathbf{Z}/k\mathbf{Z} \setminus \{0\} \to \mathbf{Z}/k\mathbf{Z} \setminus \{0\}$ which takes x to nx is one-to-one; and thus it is also onto. It follows that n is invertible modulo k. Therefore, $\gcd(n, k) = 1$. □

2. Strong Kronecker polynomials.

Examples 2.1. Let $k \in \mathbf{N} \setminus \{0,1\}$.

(1) By Theorem 1.3, k is prime if and only if

$$A_k(X) := 1 + X + \cdots + X^{k-1} \in SK[k].$$

(2) For each integer $k \geq 2$, we have $AK[k] \subseteq SK[k]$.

(3) Let m and p be nonzero natural numbers. Then, $(X^p - 1)^m$ and X^m are AK-polynomials.

(4) The product of two AK-polynomials is an AK-polynomial (that is, $AK[k]AK[s] \subseteq AK[k+s-1]$).

(5) In connection with (4), the containment $SK[k]SK[s] \subseteq SK[k+s-1]$ does not hold in general. To do so, take $P(X) := X+1$ and $Q(X) := X^2+X+1$. Then $P \in SK[2]$ and $Q \in SK[3]$; but $P(X)Q(X)$ does not divide $P(X^3)Q(X^3)$.

We need some preliminary results which will be used extensively in the next section.

We begin by some straightforward observations about polynomials.

Observation 2.2. Let $k \geq 3$ be an integer and $P(X) \in \mathbf{C}[X]$ be a polynomial of degree $k-1$. Suppose that there exists an integer $t \geq 2$ such that $P(X)$ divides $P(X^t)$. Then the following properties hold.

(1) Let λ be a nonzero root of $P(X)$. Then λ is a root of unity. In particular, $|\lambda| = 1$ (so, $P(X)$ is a Kronecker polynomial).

(2) If λ is a real root of $P(X)$, then $\lambda \in \{-1, 0, 1\}$.

Proof. (1) Since $P(X)$ divides $P(X^t)$, we deduce that λ^{t^n} is a root of $P(X)$ for each $n \in \mathbf{N}$. Since $P(X)$ has at most $k-1$ roots, there exist $n \neq m$ in $\mathbf{N}$ such that $\lambda^{t^n} = \lambda^{t^m}$. Hence there is a non zero integer $d(\lambda)$ such that $\lambda^{d(\lambda)} = 1$; and consequently, $|\lambda| = 1$.

(2) Follows immediately from the fact that if $\lambda \neq 0$, then $|\lambda| = 1$. □

Observation 2.3. Let $P(X) \in \mathbf{R}[X]$ be a monic polynomial of odd degree. Suppose that $P(X)$ divides $P(X^3)$; then $P(X)$ vanishes on one of the following points: -1, 0 and 1.

Proof. (a) If P is a polynomial of degree 1, then $P(X) = X - a$, for some real number a. As a^3 is also a root of $P(X)$, then $a^3 = a$. Thus $a \in \{-1, 0, 1\}$.

(b) If $P(X)$ is a polynomial of degree ≥ 3, then it is well known that $P(X)$ has at least one real root. Finally, according to Observation 2.2, P vanishes on 0 or 1 or -1. $\square$

Now, let us shed some light on polynomials $P(X) \in SK[k]$, when k is even.

Theorem 2.4. *Let $k \geq 4$ be an even natural number and $P(X) \in SK[k]$. Then $P(0) = 0$ or $P(1) = 0$.*

Proof. Suppose that $P(0) \neq 0$ and $P(1) \neq 0$. Let $\lambda \in \mathbf{C}$ be a root of $P(X)$. Then λ, $\lambda^2, \dots, \lambda^{k-1}$ are $k-1$ pairwise distinct roots of $P(X)$. As λ^2 is also a root of $P(X)$, we deduce that

$$\{\lambda, \lambda^2, \dots, \lambda^{k-1}\} = \{\lambda^2, \lambda^4, \dots, \lambda^{2(k-1)}\}.$$

Hence, $\lambda^{k-1} = \lambda^{2t}$, for some $1 \leq t \leq k-1$. Thus, we have $|2t - (k-1)| \leq k-1$. But, since 1 is not a root of $P(X)$ and $\lambda^{|2t-(k-1)|} = 1$, we get $|2t - (k-1)| = 0$; which contradicts the fact that k is even. $\square$

The case "k is odd" is illustrated by the following result.

Theorem 2.5. *Let $k \geq 3$ be an odd natural number and $P(X) \in SK[k]$. Then the following statements are equivalent*:

(i) $P(0) \neq 0$ *and* $P(1) \neq 0$;

(ii) k *is prime and* $P(X) = A_k(X)$.

Proof. The implication (ii) $\Longrightarrow$ (i) is straightforward.

Conversely, suppose that $P(0) \neq 0$ and $P(1) \neq 0$, and let $\lambda \in \mathbf{C}$ be a root of $P(X)$. Then, as in the proof of Theorem 2.4, we have

$$\{\lambda, \lambda^2, \dots, \lambda^{k-1}\} = \{\lambda^2, \lambda^4, \dots, \lambda^{2(k-1)}\}.$$

Hence, $\lambda^{k-2} = \lambda^{2t}$, for some $1 \leq t \leq k-1$.

The idea consists in proving that $t = k-1$. Suppose that $t \neq k-1$; then $1 \leq t \leq k-2$; so that $|2t-(k-2)| \leq k-2$. But, since $\lambda^{|2t-(k-2)|} = 1$ and 1 is not a root of $P(X)$, we get $|2t-(k-2)| = 0$; this contradicts the fact that k is odd.

It follows that $t = k-1$; and consequently, $\lambda^k = 1$. Thus, $P(X) = A_k(X)$.

By hypothesis, we have $A_k(X) = P(X) \in SK[k]$; so that k is prime, by Theorem 1.3. □

Looking at Theorem 2.4 and Theorem 2.5, one may try determining polynomials $P(X) \in SK[k]$ which do not vanish on 1; that is the aim of the following result.

Theorem 2.6. *Let $k \geq 3$ be a natural number and $P(X) \in SK[k]$ be such that $P(1) \neq 0$. Then the following properties hold.*

(i) *If k is prime, then $P(X) = A_k(X)$ or $P(X) = X^{k-1}$.*

(ii) *If k is not prime, then $P(X) = X^{k-1}$.*

Proof. Let us write $P(X) = X^i Q(X)$, with $Q(X) \in \mathbf{Z}[X]$ and $Q(0) \neq 0$. Then, clearly, $Q(X) \in SK[k-i]$. Three cases are to be considered.

Case 1: $i = 0$**.** In this case, $P(X)$ does not vanish on 0 and 1. Hence k is prime and $P(X) = A_k(X)$, by Theorem 2.4 and Theorem 2.5.

Case 2: $i \neq 0$ **and** $k - i \geq 3$**.** We will show that this case cannot happen. Indeed, since $Q(X) \in SK[k-i]$ and $Q(X)$ does not vanish on 0 and 1, we conclude that $p := k-i$ is prime and $Q(X) = A_p(X)$, by Theorem 2.4 and Theorem 2.5. Thus $P(X) = X^{k-p}A_p(X)$. But, since $P(X)$ divides $P(X^p)$, we deduce that $A_p(X)$ divides $A_p(X^p)$. This yields a contradiction, by Proposition 1.4.

Case 3: $i \neq 0$ **and** $k - i < 3$**.** In this case $k - i \in \{1, 2\}$.

(a) Suppose that $k - i = 1$, then $P(X) = X^{k-1}$.

(b) If we suppose that $k - i = 2$, then $P(X) = X^{k-2}Q(X)$. Hence $Q(X) = X - \lambda$, where $\lambda \in \mathbf{Z}$. Since λ^2 is a root of $P(X)$, we get $\lambda^2 \in \{0, \lambda\}$. It follows that $\lambda \in \{0, 1\}$; which contradicts the fact that

$Q(0) \neq 0$ and $P(1) \neq 0$. Therefore, the eventuality "$k - i = 2$" cannot happen.

As a conclusion, one may write:

(i) If k is prime, then $P(X) \in \{A_k(X), X^{k-1}\}$;

(ii) If k is not prime, then $P(X) = X^{k-1}$. □

Recall that the reciprocal $P^*(X)$ of a polynomial $P(X)$ of degree n is defined by $P^*(X) := X^n P(1/X)$. A polynomial is called *self-reciprocal* if it coincides with its reciprocal. The polynomial $P(X)$ is said to be *anti-reciprocal* if $P(X) = -P^*(X)$.

Before providing further information about SK-polynomials (for $k \geq 3$), let us state two technical lemmata. The following one may be well known; but for the sake of completeness, we include its proof.

Lemma 2.7. *Let $k \geq 3$ be an integer and $P(X) \in \mathbf{R}[X]$ a monic polynomial of degree $k - 1$. Suppose that all roots of $P(X)$ are on the unit circle. Then the following properties hold*:

(a) $P(0)^2 = 1$ *and $P(X)$ is either self-reciprocal or anti-reciprocal.*

(b) *If $P(0) = (-1)^k$, then $P(-1) = 0$.*

Proof. (1) (a). Let $\lambda_1, \lambda_2, \dots, \lambda_{k-1}$ be in $\mathbf{C}$ such that $P(X) = \prod_{i=1}^{k-1}(X - \lambda_i)$. Since $P(X) \in \mathbf{R}[X]$, we have $P(X) = \prod_{i=1}^{k-1}(X - \overline{\lambda_i})$.

On the one hand, we have

$$P^*(X) = \prod_{i=1}^{k-1}(1 - \lambda_i X) = \prod_{i=1}^{k-1}(-\lambda_i) \cdot \prod_{i=1}^{k-1}(X - \overline{\lambda_i}) = P(0)P(X)$$

and on the other hand, $P^*(X) = 1 + a_{k-2}X + \cdots + a_0 X^{k-1}$, where a_i is the coefficient of X^i in $P(X)$. Thus, $P(0)^2 = 1$, and consequently, $P(X)$ is either self-reciprocal or anti-reciprocal.

(b) As $P^*(X) = P(0)P(X)$ (according to (a)), we have $(-1)^{k-1}P(-1) = (-1)^k P(-1)$. This leads to $P(-1) = 0$. □

Combining the previous lemma and Observation 2.2, we easily get the following.

Lemma 2.8. *Let $k \geq 3$ be an integer and $P(X) := a_0 + a_1 X + \cdots + a_{k-2}X^{k-2} + X^{k-1}$ a monic polynomial in $\mathbf{R}[X]$ with degree $k-1$ such that $a_0 \neq 0$. Suppose that there exists an integer $t \geq 2$ such that $P(X)$ divides $P(X^t)$. Then $P(X)$ is either self-reciprocal or anti-reciprocal.*

The following result follows, trivially, from Theorem 2.6, Lemmas 2.7 and 2.8.

Theorem 2.9. *Let $k \geq 3$ be an integer and $P(X)$ an SK-polynomial with degree $k-1$. Then the following properties hold.*

(1) *If $P(0) = 0$ and $P(X) \neq X^{k-1}$, then $P(1) = 0$.*

(2) $P(0) \in \{-1, 0, 1\}$.

(3) *If $P(0) \neq 0$, then $P(X)$ is either self-reciprocal or anti-reciprocal.*

(4) *If $P(0) = (-1)^k$, then $P(-1) = P(1) = 0$.*

Remark 2.10. According to the above result, if $P(X) = a_i X^i + \cdots + X^{k-1}$ is an SK-polynomial such that $k \geq i+3$, then $a_i \in \{0, 1, -1\}$ (since $(P(X)/X^i) \in SK[k-i]$).

3. Absolutely Kronecker polynomials. We begin by a remark about AK-polynomials.

Remark 3.1. Let $k \geq 2$ be an integer and $P(X) \in AK[k]$. Then $P(X)$ vanishes on 0 or 1.

Indeed the result holds for each polynomial $P(X) \in SK[k]$, such that $P(X)$ divides $P(X^k)$: Suppose that 0 and 1 are not roots of P. Let $\lambda \in \mathbf{C}\backslash\{0,\ 1\}$ be a root of $P(X)$. Then $\lambda, \lambda^2, \ldots, \lambda^k$ are k distinct roots of $P(X)$, a contradiction (since $P(X)$ is of degree $k-1$). Therefore, 0 or 1 is a root of $P(X)$.

Notation 3.2. Let λ be a root of a polynomial $P(X)$; we denote by $\mathfrak{m}_{P(X)}(\lambda)$ the multiplicity of λ relatively to P.

The following lemma is needed.

Lemma 3.3. *If λ is a nonzero root of some $P \in SK[k]$, then there exists an $i \in \{1, 2, \dots, k\}$ such that $\lambda^i = 1$.*

Proof. By Observation 2.2 (1), the order of λ in the multiplicative group $\mathbf{C}^*$ is finite; let p be this order. Suppose that $p > k$; then λ, $\lambda^2, \dots, \lambda^{k-1}$ are $k-1$ distinct roots of P; and consequently, $P(0) \neq 0$ and $P(1) \neq 0$. Hence, $P(X) = A_k(X)$, by Theorems 2.4 and 2.5. Thus $\lambda^k = 1$, contradicting the fact that the order of λ is $> k$.

It follows that there exists an $i \in \{1, 2, \dots, k\}$ such that $\lambda^i = 1$. □

Proposition 3.4. *Let $P(X) \in SK[k]$ be such that $P(X) \neq A_k(X)$. If λ is a nonzero root of $P(X)$, then $\mathfrak{m}_{P(X)}(\lambda^t) \geq \mathfrak{m}_{P(X)}(\lambda)$, for each integer t.*

Proof. Let p be the order of λ. It is sufficient to prove the result for $t \in \{1, 2, \dots, p\}$. Note that this result is trivial if $t = 1$ or $\lambda = 1$. We may, thus, suppose that $t \neq 1$ and $\lambda \neq 1$. Also, we have already seen that $p \leq k$ (see Lemma 3.3).

In fact, in our case, we have $p < k$; indeed, if $p = k$, then $\lambda, \lambda^2, \dots, \lambda^{p-1}$ are distinct roots of $P(X)$, hence $P(X) = A_k(X)$, a contradiction. We may suppose that $2 \leq t \leq p \leq k-1$. Set $m_1 = \mathfrak{m}_{P(X)}(\lambda)$ and $m_t = \mathfrak{m}_{P(X)}(\lambda^t)$; then we have $P(X) = (X-\lambda)^{m_1}(X-\lambda^t)^{m_t}Q(X)$, where $Q(\lambda) \neq 0$ and $Q(\lambda^t) \neq 0$. Thus $P(X^t) = (X^t - \lambda)^{m_1}(X^t - \lambda^t)^{m_t}Q(X^t)$. As $P(X)$ divides $P(X^t)$, then $(X - \lambda)^{m_1}$ divides $(X^t - \lambda)^{m_1}(X^t - \lambda^t)^{m_t}Q(X^t) = (X^t - \lambda)^{m_1}(X - \lambda)^{m_t}H(X)Q(X^t)$, where $H(X) = X^{t-1} + X^{t-2}\lambda + \dots + X\lambda^{t-2} + \lambda^{t-1}$. But each of the following polynomials $(X^t - \lambda)^{m_1}$, $Q(X^t)$ and $H(X)$ does not vanish at λ. Therefore, $(X-\lambda)^{m_1}$ divides $(X-\lambda)^{m_t}$, and consequently, $m_1 \leq m_t$. □

Remarks 3.5. (1) If k is a prime number and $P(X) = A_k(X)$, then $P(X) \in SK[k]$. Let λ be a root of P(X). Then $o(\lambda) = k$ and any other root $\lambda^t (1 \leq t \leq k-1)$ has order k; moreover, $\mathfrak{m}_{P(X)}(\lambda^t) = \mathfrak{m}_{P(X)}(\lambda) = 1$, for each $t \in \{1, 2, \dots, k-1\}$.

(2) The inequality $\mathfrak{m}_{P(X)}(\lambda^t) \geq \mathfrak{m}_{P(X)}(\lambda)$ in Proposition 3.4 may be an equality. Indeed, if λ is a root of $P(X)$ of order p and $t \in \{1, 2, \dots, p-1\}$ is such that $o(\lambda) = o(\lambda^t) = p$, then $\{\lambda, \lambda^2, \dots, \lambda^{p-1}\} =$

$\{\lambda^t, (\lambda^t)^2, \ldots, (\lambda^t)^{p-1}\}$. Thus, according to Proposition 3.4, we have $\mathfrak{m}_{P(X)}(\lambda^t) \geq \mathfrak{m}_{P(X)}(\lambda)$ and $\mathfrak{m}_{P(X)}(\lambda) \geq \mathfrak{m}_{P(X)}(\lambda^t)$. Therefore, $\mathfrak{m}_{P(X)}(\lambda^t) = \mathfrak{m}_{P(X)}(\lambda)$.

Proposition 3.6. *Let $P(X) \in SK[k]$ be such that $P(X) \neq A_k(X)$. If λ is a nonzero root of $P(X)$ of order p, then for each $n \geq 1$, the following properties hold.*

(i) *λ is a root of $P(X^n)$.*

(ii) *$\mathfrak{m}_{P(X^n)}(\lambda) = \mathfrak{m}_{P(X)}(\lambda^r)$ where r is the remainder of the Euclidian division of n by p.*

Proof. We consider two cases.

Case 1. Suppose that $p = 1$. In this case, $\lambda = 1$ and $P(X)$ has the following form $P(X) = (X-1)^s Q(X)$, where $s = \mathfrak{m}_{P(X)}(1)$ and $Q(1) \neq 0$. As $P(X^n) = (X^n - 1)^s Q(X^n)$ and $Q(1^n) = Q(1) \neq 0$, then $\mathfrak{m}_{P(X^n)}(1) = \mathfrak{m}_{P(X)}(1)$.

Case 2. Let us suppose that $o(\lambda) = p \geq 2$. As in the proof of Proposition 3.4, we have $o(\lambda) = p \leq k-1$ and $\lambda, \lambda^2, \ldots, \lambda^p$ are distinct roots of $P(X)$. Set $m_t = \mathfrak{m}_{P(X)}(\lambda^t)$ for each $t \in \{1, 2, \ldots, p\}$; then $P(X)$ has the following form

$$P(X) = (X-\lambda)^{m_1}(X-\lambda^2)^{m_2}\cdots(X-\lambda^p)^{m_p}Q(X),$$

where $Q(\lambda^t) \neq 0$ for each $t \in \{1, 2, \ldots, p\}$. Writing the Euclidian division of n by p, we get $n = qp + r$, where r is an integer such that $0 \leq r < p$. Thus $\lambda^n = \lambda^r \in \{\lambda, \lambda^2, \ldots \lambda^p\}$ and

$$\begin{aligned} P(X^n) &= (X^n-\lambda)^{m_1}(X^n-\lambda^2)^{m_2}\cdots(X^n-\lambda^r)^{m_r} \\ &\qquad \cdots(X^n-\lambda^p)^{m_p}Q(X^n) \\ &= (X^n-\lambda)^{m_1}(X^n-\lambda^2)^{m_2}\cdots(X^n-\lambda^n)^{m_r} \\ &\qquad \cdots(X^n-\lambda^p)^{m_p}Q(X^n) \\ &= (X-\lambda)^{m_r}R(X), \end{aligned}$$

where

$$R(X) = Q(X^n)(X^{n-1} + X^{n-2}\lambda + \cdots + X\lambda^{n-2} + \lambda^{n-1})^{m_r} \prod_{\substack{t=1 \\ t\neq r}}^{p}(X^n-\lambda^t)^{m_t}.$$

As

$$R(\lambda) = Q(\lambda^n)(n\lambda^{n-1})^{m_r} \prod_{\substack{t=1\\ t\neq r}}^{p} (\lambda^n - \lambda^t)^{m_t} = Q(\lambda^r)(n\lambda^{n-1})^{m_r} \prod_{\substack{t\neq r\\ t=1}}^{p} (\lambda^n - \lambda^t) \neq 0,$$

we have $\mathfrak{m}_{P(X^n)}(\lambda) = m_r = \mathfrak{m}_{P(X)}(\lambda^r)$. □

The following results clarify the links between the two sets $SK[n]$ and $AK[n]$.

Theorem 3.7. *Let $k \geq 3$ be an integer.*

(i) *If k is prime, then $AK[k] = SK[k] \setminus \{A_k(X)\}$.*

(ii) *If k is composite, then $AK[k] = SK[k]$.*

Proof. Let $P(X) \in SK[k] \setminus \{A_k(X)\}$. We will prove that $P(X)$ divides $P(X^n)$ for each integer $n \geq 1$. By definition, $P(X)$ divides $P(X^n)$ for each integer n such that $1 \leq n \leq k-1$. Let us suppose that $n \geq k$. To show that $P(X)$ divides $P(X^n)$, it suffices to show that each root λ of $P(X)$ is also a root of $P(X^n)$ and $\mathfrak{m}_{P(X^n)}(\lambda) \geq \mathfrak{m}_{P(X)}(\lambda)$. Two cases have to be considered:

Case 1. Suppose that $\lambda = 0$. Then $P(X) = X^s Q(X)$, where $s = \mathfrak{m}_{P(X)}(0)$ and $Q(0) \neq 0$. As $P(X^n) = X^{ns}Q(X^n)$, then 0 is a root of $P(X^n)$ and $\mathfrak{m}_{P(X^n)}(0) = n\mathfrak{m}_{P(X)}(0) > \mathfrak{m}_{P(X)}(0)$.

Case 2. Suppose that $\lambda \neq 0$ and $o(\lambda) = p$. Then, according to Proposition 3.6, λ is a root of $P(X^n)$ and $\mathfrak{m}_{P(X^n)}(\lambda) = \mathfrak{m}_{P(X)}(\lambda^t)$ for some $t \in \{0, 1, \dots, p-1\}$. Now, by Proposition 3.4, we have $\mathfrak{m}_{P(X)}(\lambda^t) \geq \mathfrak{m}_{P(X)}(\lambda)$. It follows that $\mathfrak{m}_{P(X^n)}(\lambda) \geq \mathfrak{m}_{P(X)}(\lambda)$. □

Corollary 3.8. *Let $P(X)$ be a polynomial such that $P(X) = X^s Q(X)$ with $Q(0) \neq 0$, $s \geq 1$ and $k \geq 2 + s$. Then $P(X) \in SK[k]$ if and only if $Q(X) \in AK[k-s]$.*

Proof. Set $m = k - s$. Then, by Remark 2.10, $Q(X) \in SK[m]$. According to Theorem 3.7, to prove that $Q(X) \in AK[m]$, it suffices to show that $Q(X) \neq A_m(X)$. Suppose that $Q(X) = A_m(X)$. Since $m \leq k-1$, $P(X)$ divides $P(X^m)$, so $P(X^m) = P(X)F(X)$ for some polynomial $F(X) \in \mathbf{Z}[X]$. As $P(X) = X^s A_m(X)$, we get $X^{ms-s}A_m(X^m) = A_m(X)F(X)$. Thus $A_m(X)$ divides $A_m(X^m)$, a contradiction with Proposition 1.4. □

Now, we are in a position to state our main result. First, let us remark that, according to Theorem 3.7 and Corollary 3.8, in order to know polynomials $P(X) \in SK[k]$ it is enough to detect polynomials $P(X) \in AK[k]$ such that $P(0) \neq 0$.

Theorem 3.9. *Let $k \geq 2$ be an integer and $AK^0[k]$ the set of polynomials $P(X) \in AK[k]$ such that $P(0) \neq 0$. Then the following statements are equivalent*:

(1) $P \in AK^0[k]$;

(2) *there exist integers $\alpha_1, \alpha_2, \dots, \alpha_{k-1} \geq 0$ such that*

$$P(X) = \prod_{i=1}^{k-1} (\phi_i(X))^{\alpha_i},$$

with $k-1 = \sum_{i=1}^{k-1} \alpha_i \varphi(i)$; and if i divides j, then $\alpha_i \geq \alpha_j$.

Proof. (1) $\Rightarrow$ (2). Let $P \in AK^0[k]$. Then, according to Proposition 1.4, $P \neq A_k(X)$. Let λ be a root of P. Then λ is of order $l \in \{1, 2, \dots, k-1\}$ (since $P \neq A_k(X)$). Now, if μ is a root of the lth cyclotomic polynomial $\phi_l(X)$, then μ is also a root of P and $\mathfrak{m}_{P(X)}(\mu) = \mathfrak{m}_{P(X)}(\lambda)$ (by Remark 3.5 (2)). Hence, denoting $\alpha_l := \mathfrak{m}_{P(X)}(\lambda)$, we see that $(\phi_l(X))^{\alpha_l}$ divides $P(X)$.

For each $i \in \{1, 2, \dots, k-1\}$, let α_i be the integer defined by:

(a) $\alpha_i = 0$, if there is no root of P of order i;

(b) if P has a root of order i, then we let α_i be the multiplicity of that root relative to P (the multiplicity depends only on the order of the root; Remark 3.5 (2)).

Under the above notations, we have proved that $\prod_{i=1}^{k-1}(\phi_i(X))^{\alpha_i}$ divides $P(X)$; and since the two polynomials are monic, it suffices to show that $P(X)$ divides $\prod_{i=1}^{k-1}(\phi_i(X))^{\alpha_i}$ to get the equality. Indeed, let λ be a root of P with multiplicity m. Let l denotes the order of λ, then $(X-\lambda)^m$ divides $(\phi_l(X))^m$, proving that $P(X)$ divides the polynomial $\prod_{i=1}^{k-1}(\phi_i(X))^{\alpha_i}$.

Note that the previous equality is a direct consequence of Lemma 3.3, Proposition 3.4 and the canonical form of Kronecker polynomials provided by Damianou in [**3**]; but, here we have proved it using our own results to make the paper as self contained as possible.

To end the current implication, we prove that, if $i, j \in \{1, 2, \dots, k-1\}$ such that i divides j, then $\alpha_i \geq \alpha_j$.

Indeed, there exists an integer s such that $j = is$. Clearly, α_j may be assumed a nonzero integer. In this case, there exists a root λ of P such that $o(\lambda) = j$ and $\mathfrak{m}_{P(X)}(\lambda) = \alpha_j$. Hence, λ^s is a root of P of order i; so that $\mathfrak{m}_{P(X)}(\lambda^s) = \alpha_i$. But, by Proposition 3.4, $\mathfrak{m}_{P(X)}(\lambda^s) \geq \mathfrak{m}_{P(X)}(\lambda) = \alpha_j$; this gives immediately $\alpha_i \geq \alpha_j$.

(2) $\Rightarrow$ (1). Let $P(X) = \prod_{i=1}^{k-1}(\phi_i(X))^{\alpha_i}$, with the property that $k-1 = \sum_{i=1}^{k-1}\alpha_i\varphi(i)$; and if i divides j, then $\alpha_i \geq \alpha_j$. We have, clearly, $P(0) \neq 0$. Let us prove that $P(X) \in AK^0[k]$; that is $P(X)$ divides $P(X^n)$ for each integer $n \geq 1$. It suffices to show that for each root λ of P, λ is also a root of the polynomial $P(X^n)$ and $\mathfrak{m}_{P(X^n)}(\lambda) \geq \mathfrak{m}_{P(X)}(\lambda)$.

Let λ be a root of P; then there exists an $i \in \{1, 2, \dots, k-1\}$ such that $\phi_i(\lambda) = 0$. Hence $\mathfrak{m}_{P(X)}(\lambda) = \alpha_i \geq 1$ and $o(\lambda) = i$. Thus $\lambda^n \in \{1, \lambda, \lambda^2, \dots, \lambda^{i-1}\}$; so to prove that λ is a root of $P(X^n)$, it is sufficient to show that 1, λ, $\lambda^2, \dots, \lambda^{i-1}$ are roots of P.

Indeed, let $t \in \{1, 2, \dots, i-1\}$, then $o(\lambda^t) := d$ is a divisor of i. By hypothesis, $\alpha_d \geq \alpha_i$. Hence $\alpha_d \neq 0$. But since $\phi_d(\lambda^t) = 0$, we get $P(\lambda^t) = 0$.

Now, let us show that $\mathfrak{m}_{P(X^n)}(\lambda) \geq \alpha_i$. Let $d = o(\lambda^n)$; then d divides i. But, on the one hand, we have $\phi_d(\lambda^n) = 0$ and on the other hand we have $\alpha_d \geq \alpha_i$, showing that the multiplicity of λ relative to the polynomial $P(X^n) = \prod_{i=1}^{k-1}(\phi_i(X^n))^{\alpha_i}$ is greater than $\alpha_d \geq \alpha_i$. $\square$

4. Numerical examples. This section is devoted to some numerical examples illustrating some of theoretical results of the previous sections.

Let n be an integer such that $n \geq 2$. We denote by $SK[n]$ the set of all strong Kronecker polynomials of degree $n-1$, the cardinality of $SK[n]$ will be denoted by $\mathcal{SK}(n)$. We, also, denote by $AK[n]$ the set of all absolutely Kronecker polynomials of degree $n-1$; the cardinality of $AK[n]$ will be denoted by $\mathcal{AK}(n)$. The set of all polynomials $P(X) \in AK[n]$ such that $P(0) \neq 0$ will be denoted by $AK^0[n]$; and $\mathcal{AK}^0(n)$ will denote its cardinality.

As a direct consequence of our theoretical study of strong (respectively absolutely) Kronecker polynomials we have the following properties:

(1) $SK[n] = AK[n]$, if n is composite.

(2) $SK[n] = AK[n] \cup \{A_n(X)\}$, if n is an odd prime.

(3) $AK[n] = \cup_{i=0}^{n-1} X^i AK^0[n-i]$, where

$$X^i AK^0[n-i] := \{X^i f : f \in AK^0[n-i]\} \quad \text{and} \quad AK^0[1] = \{1\}.$$

(4) $\mathcal{SK}(n) = \mathcal{AK}(n)$, if n is composite; and $\mathcal{SK}(n) = \mathcal{AK}(n) + 1$, if n is an odd prime number.

(5) $SK[2] = \{X + a : a \in \mathbf{Z}\}$ and $AK[2] = \{X, X-1\}$.

(6) $\mathcal{AK}(n) = \sum_{i=0}^{n-1} \mathcal{AK}^0(n-i) = \sum_{i=1}^{n} \mathcal{AK}^0(i)$.

In the following data the polynomial $P(X) = \prod_{i=1}^{n-1} (\phi_i(X))^{\alpha_i}$ with degree $n-1$ will be denoted by $(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$.

If we would like to check by hand the polynomials in question, the following list of cyclotomic polynomials will be useful:

(1) $\phi_1(X) = X - 1$,

(2) $\phi_2(X) = X + 1$,

(3) $\phi_3(X) = X^2 + X + 1$,

(4) $\phi_4(X) = X^2 + 1$,

(5) $\phi_5(X) = X^4 + X^3 + X^2 + X + 1$,

(6) $\phi_6(X) = X^2 - X + 1$,

(7) $\phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$,

(8) $\phi_8(X) = X^4 + 1$,

(9) $\phi_9(X) = X^6 + X^3 + 1$,

(10) $\phi_{10}(X) = X^4 - X^3 + X^2 - X + 1$.

TABLE 1. Elements of $AK^0[n]$ for $n \in \{2, 3, 4, 5, 6\}$.

n	2	3	4	5	6
Elements of $AK^0[n]$	(1)	(1,1)	(1,0,1)	(1,1,0,1)	(1,0,0,0,1)
		(2,0)	(2,1,0)	(1,1,1,0)	(2,1,0,1,0)
			(3,0,0)	(2,0,1,0)	(2,1,1,0,0)
				(2,2,0,0)	(3,0,1,0,0)
				(3,1,0,0)	(3,2,0,0,0)
				(4,0,0,0)	(4,1,0,0,0)
					(5,0,0,0,0)

TABLE 2. Elements of $AK^0[7]$ and $AK^0[8]$.

n	7	8
Elements of $AK^0[n]$	(1,1,0,0,1,0)	(1,0,1,0,1,0,0)
	(1,1,1,0,0,1)	(2,1,0,0,1,0,0)
	(1,1,1,1,0,0)	(2,1,1,0,0,1,0)
	(2,0,0,0,1,0)	(2,1,1,1,0,0,0)
	(2,0,2,0,0,0)	(2,1,2,0,0,0,0)
	(2,2,0,1,0,0)	(3,0,0,0,1,0,0)
	(2,2,1,0,0,0)	(3,0,2,0,0,0,0)
	(3,1,0,1,0,0)	(3,2,0,1,0,0,0)
	(3,1,1,0,0,0)	(3,2,1,0,0,0,0)
	(3,3,0,0,0,0)	(4,1,0,1,0,0,0)
	(4,0,1,0,0,0)	(4,1,1,0,0,0,0)
	(4,2,0,0,0,0)	(4,3,0,0,0,0,0)
	(5,1,0,0,0,0)	(5,0,1,0,0,0,0)
	(6,0,0,0,0,0)	(5,2,0,0,0,0,0)
		(6,1,0,0,0,0,0)
		(7,0,0,0,0,0,0)

TABLE 3. Elements of $AK^0[9]$ and $AK^0[10]$.

n	9	10
Elements of $AK^0[n]$	(1,1,0,0,0,0,1,0)	(1,0,1,0,0,0,0,0,1)
	(1,1,0,1,0,0,0,1)	(1,0,1,0,0,0,1,0,0)
	(1,1,0,1,1,0,0,0)	(2,1,0,0,0,0,1,0,0)
	(1,1,1,0,1,0,0,0)	(2,1,0,1,0,0,0,1,0)
	(1,1,1,1,0,1,0,0)	(2,1,0,1,1,0,0,0,0)
	(2,0,0,0,0,0,1,0)	(2,1,1,0,1,0,0,0,0)
	(2,0,1,0,1,0,0,0)	(2,1,1,1,0,1,0,0,0)
	(2,2,0,0,1,0,0,0)	(2,1,2,0,0,1,0,0,0)
	(2,2,0,2,0,0,0,0)	(2,1,2,1,0,0,0,0,0)
	(2,2,1,0,0,1,0,0)	(3,0,0,0,0,0,1,0,0)
	(2,2,1,1,0,0,0,0)	(3,0,1,0,1,0,0,0,0)
	(2,2,2,0,0,0,0,0)	(3,0,3,0,0,0,0,0,0)
	(3,1,0,0,1,0,0,0)	(3,2,0,0,1,0,0,0,0)
	(3,1,1,0,0,1,0,0)	(3,2,0,2,0,0,0,0,0)
	(3,1,1,1,0,0,0,0)	(3,2,1,0,0,1,0,0,0)
	(3,1,2,0,0,0,0,0)	(3,2,1,1,0,0,0,0,0)
	(3,3,0,1,0,0,0,0)	(3,2,2,0,0,0,0,0,0)
	(3,3,1,0,0,0,0,0)	(4,1,0,0,1,0,0,0,0)
	(4,0,0,0,1,0,0,0)	(4,1,1,0,0,1,0,0,0)
	(4,0,2,0,0,0,0,0)	(4,1,1,1,0,0,0,0,0)
	(4,2,0,1,0,0,0,0)	(4,1,2,0,0,0,0,0,0)
	(4,2,1,0,0,0,0,0)	(4,3,0,1,0,0,0,0,0)
	(4,4,0,0,0,0,0,0)	(4,3,1,0,0,0,0,0,0)
	(5,1,0,1,0,0,0,0)	(5,0,0,0,1,0,0,0,0)
	(5,1,1,0,0,0,0,0)	(5,0,2,0,0,0,0,0,0)
	(5,3,0,0,0,0,0,0)	(5,2,0,1,0,0,0,0,0)
	(6,0,1,0,0,0,0,0)	(5,2,1,0,0,0,0,0,0)
	(6,2,0,0,0,0,0,0)	(5,4,0,0,0,0,0,0,0)
	(7,1,0,0,0,0,0,0)	(6,1,0,1,0,0,0,0,0)
	(8,0,0,0,0,0,0,0)	(6,1,1,0,0,0,0,0,0)
		(6,3,0,0,0,0,0,0,0)
		(7,0,1,0,0,0,0,0,0)
		(7,2,0,0,0,0,0,0,0)
		(8,1,0,0,0,0,0,0,0)
		(9,0,0,0,0,0,0,0,0)

The following data gives the values of the counting functions $\mathcal{AK}(n)$, $\mathcal{AK}^0(n)$ and $\mathcal{SK}(n)$ for $3 \le n \le 20$.

n	$\mathcal{SK}(n)$	$\mathcal{AK}(n)$	$\mathcal{AK}^0(n)$
3	5	4	2
4	7	7	3
5	14	13	6
6	20	20	7
7	35	34	14
8	50	50	16
9	80	80	30
10	115	115	35
11	177	176	61
12	243	243	67
13	362	361	118
14	494	494	133
15	705	705	211
16	944	944	239
17	1330	1329	385
18	1750	1750	421
19	2414	2413	663
20	3145	3145	732

We close this paper by stating some problems.

Problem 4.1. *Determine the generating functions of* $\mathcal{AK}(n)$, $\mathcal{AK}^0(n)$ *and* $\mathcal{SK}(n)$, *that is, the functions:*

$$\sum_{n=1}^{\infty} \mathcal{AK}^0(n)x^n, \ \sum_{n=1}^{\infty} \mathcal{AK}(n)x^n, \ \sum_{n=3}^{\infty} \mathcal{SK}(n)x^n.$$

Problem 4.2. *Determine the asymptotic behavior of the counting functions* $\mathcal{AK}(n)$, $\mathcal{AK}^0(n)$ *and* $\mathcal{SK}(n)$.

Problem 4.3. *Find an algorithm determining the set* $AK^0[n]$.

Acknowledgments. The authors thank the anonymous referee for his/her very valuable and helpful advice, corrections and remarks.

REFERENCES

1. D. Caragea and V. Ene, *Problems and solutions*: *Problems*: 10802, Amer. Math. Monthly **107** (2000), 462.

2. D. Caragea, V. Ene, D. Alvis and N. Komanda, *Problems and solutions*: *Solutions*: 10802, Amer. Math. Monthly **109** (2002), 570–571.

3. P.A. Damianou, *Monic polynomials in* $\mathbf{Z}[X]$ *with roots in the unit disc*, Amer. Math. Monthly **108** (2001), 253–257.

4. L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, Crelle, Oeuvres **I** (1857), 105–108.

5. J.H. Nieto, *On the divisibility of polynomials with integer coefficients*, Divulg. Mat. **11** (2003), 149–152 (in Spanish).

University of Sanaá, Faculty of Science, Department of Mathematics, P.O. Box 12460, Sanaá, Yemen
Email address: aaayache@yahoo.com

King Fahd University of Petroleum and Minerals, Department of Mathematics & Statistics, P.O. Box 5046, Dhahran 31261, Saudi Arabia
Email address: othechi@yahoo.com, othechi@math.com

Department of Mathematics, Faculty of Sciences of Tunis, University Tunis-El Manar, "Campus Universitaire" 2092 El Manar, Tunis, Tunisia
Email address: mongi.naimi@fst.rnu.tn