ZSIGMONDY'S THEOREM FOR CHEBYSHEV POLYNOMIALS

STEFAN BARAŃCZUK

Abstract. For every natural number $a > 1$ consider the sequence $(T_n(a) - 1)_{n=1}^{\infty}$ defined by Chebyshev polynomials T_n. We list all pairs (n, a) for which the term $T_n(a) - 1$ has no primitive prime divisor.

There is an intriguing link between the sequence of the power maps x^n and the sequence of the Chebyshev polynomials $T_n(x)$, defined either by the property $T_n(\cos(\theta)) = \cos(n\theta)$, or recursively $T_0(x) = 1$, $T_1(x) = x$, $T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x)$ (our reference for the Chebyshev polynomials is [Riv]). For example, they both satisfy the composition identity, which we state here for the Chebyshev polynomials:

$$T_n(T_m(x)) = T_m(T_n(x)) = T_{mn}(x).$$

Furthermore, the celebrated Julia-Ritt result says that if two polynomials commute under composition, then either both are iterates of the same polynomial, or both are in a sense similar to either Chebyshev polynomials or power maps.

There are also number theoretic properties shared by both sequences (see Section 5.3. in [Riv]). In this paper we investigate such property – namely, we prove the Chebyshev polynomials analogue of Zsigmondy's Theorem.

Zsigmondy's Theorem says for which natural numbers $a, n > 1$ there is a prime divisor p of $a^n - 1$ that does not divide any of the numbers $a^d - 1$, $d < n$ (such primes are called *primitive prime divisors*) or equivalently, there is a prime number p such that the multiplicative order $\mathrm{ord}_p(a)$ equals n.

The above mentioned similarities evoke the question whether we could replace a^n in Zsigmondy's Theorem by $T_n(a)$. Our answer is as follows. Denote by $\mathrm{Che}_p(x)$ the minimal positive integer m such that $T_m(x) \equiv 1 \mod p$; this quantity is the Chebyshevian analogue of the multiplicative order (this claim is justified by Lemmas 3 and 4).

Theorem 1. *Let $a, n > 1$ be natural numbers. There exits a prime number p such that $n = \mathrm{Che}_p(a)$, except in the following cases:*

- $n = 2$ *and* $a = 2^\alpha - 1$,
- $n = 3$ *and* $a = \frac{3^\alpha - 1}{2}$,
- $n = 4$ *and* $a = 2^\alpha$,
- $n = 6$ *and* $a = \frac{3^\alpha + 1}{2}$.

The proof takes as a model the *einfacher Bewais* of Zsigmondy's Theorem presented in [Lün1] (compare our Theorem 13 with Satz 1).

Proposition 2. *(Exercise 1.1.5 in* [Riv]*) If a, b are nonnegative integers, then*

$$(T_{a+b}(x) - 1)(T_{|a-b|}(x) - 1) = (T_a(x) - T_b(x))^2.$$

The following lemma is the analogue of Fermat's little theorem for Chebyshev polynomials.

Lemma 3. *Let p be an odd prime number. For every $x \in \mathbb{N}$*

$$T_{p-1}(x) \equiv 1 \mod p \quad \text{or} \quad T_{p+1}(x) \equiv 1 \mod p.$$

For every $x \in \mathbb{N}$

$$T_2(x) \equiv 1 \mod 2.$$

2010 *Mathematics Subject Classification.* 11A41.
Key words and phrases. Chebyshev polynomials; primitive prime divisors; Zsigmondy's theorem.

Proof. $T_2(x) = 2x^2 - 1$. If p is an odd prime then we have (cf. (5.32) in [Riv])

$$T_p(x) \equiv T_1(x) \mod p$$

and

$$(T_{p+1}(x) - 1)(T_{p-1}(x) - 1) = (T_p(x) - T_1(x))^2$$

by Proposition 2. □

Lemma 4. *Let p be a prime number and $x \in \mathbb{N}$. Let m be the minimal positive integer such that $T_m(x) \equiv 1 \mod p$. Then $T_n(x) \equiv 1 \mod p$ for a positive integer n if and only if $m \mid n$.*

Proof. ($\Leftarrow$) For every n we have $T_n(1) = 1$. Thus if $m \mid n$ then $T_n(x) \equiv 1 \mod p$ by the composition identity.

($\Rightarrow$) Let $r = n - km$ be the remainder obtained upon dividing n by m. Suppose $r > 0$. Putting $a = km$ and $b = r$ in Proposition 2 we get

$$(T_n(x) - 1)(T_{|km-r|}(x) - 1) = ((T_{km}(x) - 1) - (T_r(x) - 1))^2 .$$

Arguing as in the ($\Leftarrow$) part of the proof we get $T_{km}(x) - 1 \equiv 0 \mod p$. Since $T_n(x) - 1 \equiv 0 \mod p$, we have $T_r(x) - 1 \equiv 0 \mod p$ by the above identity. This contradicts the minimality of m. □

We immediately get the following.

Lemma 5. *If $x \in \mathbb{N}$ and p is an odd prime number then* $\mathrm{Che}_p(x)$ *divides $p-1$ or $p+1$. In particular,* $\mathrm{Che}_p(x)$ *and p are coprime. If x is odd then* $\mathrm{Che}_2(x) = 1$. *If x is even then* $\mathrm{Che}_2(x) = 2$.

The key tool of the proof of Zsigmondy's Theorem is the factorization of polynomials $x^n - 1$ into cyclotomic polynomials (our reference for them is [Lün2]). The following lemma describes its analogue for Chebyshev polynomials.

Lemma 6. *For every $n \geq 1$*

$$T_n(x) - 1 = \prod_{d \mid n} \Omega_d^{\sigma_d}(x)$$

where $\Omega_1(x) = x - 1$ and for $d \geq 2$

$$\Omega_d(x) = \prod_{\substack{1 \leq k \leq \frac{d}{2} \\ \gcd(k,d)=1}} 2(x - \cos \tfrac{2k\pi}{d})$$

and

$$\sigma_d = \begin{cases} 1 & \text{if } d = 1, 2, \\ 2 & \text{if } d > 2. \end{cases}$$

Proof. For every $n \geq 1$ the local maxima of $T_n(x)$ are exactly at $\cos \frac{2k\pi}{n}$, $1 \leq k < \frac{n}{2}$, and they all have value 1. Besides those points, $T_n(x) = 1$ only for $x = 1$ and arbitrary n, and for $x = -1$ and even n (see Section 1.2. in [Riv]). □

The significance of $\Omega_n(x)$ can be seen at a glance: it is exactly the factor that distinguishes $T_n(x) - 1$ from all $T_d(x) - 1$, $d \mid n$, $d < n$. Precisely speaking, if there is a primitive prime divisor of $T_n(x) - 1$, it has to divide $\Omega_n(x)$ by Lemma 10.

Proposition 7. *Let m, n be positive integers. Then $\Omega_{mn}(x)$ is a divisor of $\Omega_n(T_m(x))$. If moreover $n \geq 3$ and every prime divisor of m divides also n, then $\Omega_{mn}(x) = \Omega_n(T_m(x))$.*

Proof. Let α be any zero of $\Omega_{mn}(x)$. We have $\alpha = \cos \frac{2k\pi}{mn}$ for some k coprime to mn and $1 \leq k \leq \frac{mn}{2}$. Since $T_m(\cos(\theta)) = \cos(m\theta)$, we get $T_m(\alpha) = \cos \frac{2k\pi}{n} = \cos \frac{2(n-k)\pi}{n}$. Thus $T_m(\alpha)$ is a zero of $\Omega_n(x)$. So all zeros of $\Omega_{mn}(x)$ are zeros of $\Omega_n(T_m(x))$. Since $\Omega_{mn}(x)$ has only simple zeros, we get that $\Omega_{mn}(x)$ is a divisor of $\Omega_n(T_m(x))$.

Now suppose that $n \geq 3$ and every prime divisor of m divides also n. If $d \geq 3$ then the degree of Ω_d is $\varphi(d)/2$ and its leading coefficient is $2^{\varphi(d)/2}$. If every prime divisor of m divides also n, then

n and mn have the same set of prime divisors. Hence we get $\varphi(mn) = m\varphi(n)$ (see e.g. Satz 9.4 in [Lün2]). Thus $\Omega_{mn}(x)$ and $\Omega_n(T_m(x))$ have the same degree and the same leading coefficient. □

Proposition 8. *Let n be an odd natural number. Then $\Omega_n(0) = \pm 1$. If moreover $n \geq 3$ then $\Omega_{2n}(x) = \pm\Omega_n(-x)$.*

Proof. The proof of the first statement is by induction on n. We have $\Omega_1(x) = x - 1$, so $\Omega_1(0) = -1$. Suppose that for every odd natural number d such that $1 \leq d < n$ we have $\Omega_d(0) = \pm 1$. Now compute $-1 = T_n(0) - 1 = \prod_{d|n} \Omega_d^{\sigma_d}(0) = \Omega_1(0) \cdot \prod_{d|n,\, 1<d<n} \Omega_d^2(0) \cdot \Omega_n^2(0) = -\Omega_n^2(0)$. We get $\Omega_n^2(0) = 1$.

Now suppose $n \geq 3$. We have $\deg \Omega_{2n} = \varphi(2n)/2 = \varphi(n)/2 = \deg \Omega_n$. The same shows that Ω_{2n} and Ω_n have the same leading coefficient, namely $2^{\varphi(n)/2}$. It remains to examine the zeros. We have $-\cos \frac{2k\pi}{n} = \cos \frac{2(n-2k)\pi}{2n}$. Denote $l = n - 2k$. The conditions $1 \leq k \leq \frac{n}{2}$, $\gcd(k, n) = 1$ are equivalent to $1 \leq l \leq \frac{2n}{2}$, $\gcd(l, 2n) = 1$. Hence $\Omega_{2n}(x)$ and $\Omega_n(-x)$ have the same set of zeros. □

Proposition 9. *Let $\mathbb{K}$ be a field of characteristic 0. Suppose that $P(x) \in \mathbb{K}[x]$, $P(0) = 1$, and $P^2(x) \in \mathbb{Z}[x]$. Then $P(x) \in \mathbb{Z}[x]$.*

Proof. Put $P(x) = \sum_{i=0}^{\infty} c_i x^i$. Since the coefficient of x^k in $P^2(x)$ equals $2c_k + \sum_{0<i<k} c_i c_{k-i}$, we get by induction on k that each c_k is a rational number with denominator being a power of 2. Thus $P(x) = 1 + \frac{Q(x)}{2^e}$, where $Q(x) = \sum_{i=1}^{\infty} d_i x^i \in \mathbb{Z}[x]$ with some d_j being odd. The coefficient of x^{2j} in $Q^2(x)$ equals $d_j^2 + 2\sum_{0<i<j} d_{j+i} d_{j-i}$, so it is an odd integer. Thus the coefficient of x^{2j} in $2^{e+1}Q(x) + Q^2(x)$ is also odd. But we have $P^2(x) = 1 + \frac{2^{e+1}Q(x) + Q^2(x)}{2^{2e}}$, so $e = 0$. □

Lemma 10. $\Omega_n \in \mathbb{Z}[x]$.

Proof. First we prove the lemma for odd n. We use induction. $\Omega_1 \in \mathbb{Z}[x]$. Let $n > 1$. Suppose that for every odd natural number d such that $1 \leq d < n$ we have $\Omega_d \in \mathbb{Z}[x]$. We have $T_n(x) - 1 = \prod_{d|n} \Omega_d^{\sigma_d}(x) = \Omega_n^2(x) g(x)$, where $g(x) \in \mathbb{Z}[x]$. Put $\Omega_n^2(x) = \sum_{i=0}^{\varphi(n)} a_i x^i$ and $g(x) = \sum_{i=0}^{n-\varphi(n)} b_i x^i$. We have $a_0 = \pm 1$ and $b_0 = \pm 1$ by Proposition 8. Let $i \leq \varphi(n)$ and assume that $a_j \in \mathbb{Z}$ for every $j < i$. Since $a_i b_0 + a_{i-1} b_1 + \ldots \in \mathbb{Z}$ as the coefficient of x^i in $T_n(x) - 1$, we have $a_i \in \mathbb{Z}$. Thus $\Omega_n \in \mathbb{Z}[x]$ by Proposition 9.

We directly compute that $\Omega_2(x) = 2(x + 1)$, and $\Omega_4(x) = 2x$.

If n is the product of 2 and an odd natural number greater or equal to 3, we use Proposition 8.

Finally, we get the lemma for arbitrary even n by Proposition 7, since $\mathbb{Z}[x]$ is closed under composition. □

Proposition 11. *For every natural number n and every nonzero real number x*

$$\frac{T_n(x+1) - 1}{x} = n^2 + \frac{n^2(n^2-1)}{6}x + \frac{n^2(n^2-1)(n^2-4)}{90}x^2 + \ldots,$$

where the dots denote terms with irrelevant coefficients.

Proof. The formula

$$T_n(x+1) = 1 + n^2 x + \frac{n^2(n^2-1)}{6}x^2 + \frac{n^2(n^2-1)(n^2-4)}{90}x^3 + \ldots$$

can be proved by induction on n. □

Remark 12. One can observe that

$$T_n(x+1) = 1 + \sum_{k=1}^{n} \frac{2^k \prod_{i=0}^{k-1}(n^2 - i^2)}{(2k)!} x^k.$$

Theorem 13. *Let $a, n > 1$ be natural numbers. Let p be a prime number dividing $\Omega_n(a)$. Denote $f = \mathrm{Che}_p(a)$. There exits a nonnegative integer i such that $n = fp^i$. If $i > 0$, then p is the greatest prime divisor of n. If moreover $p^2 \mid \Omega_n(a)$ then either $p = 2$ and $n \in \{2, 4\}$, or $p = 3$ and $n \in \{3, 6\}$.*

Proof. $\Omega_n(a)$ is a divisor of $T_n(a)-1$, so $T_n(a)-1=0 \mod p$. Hence $f\mid n$ by Lemma 4, and we can write $n=fp^iw$, where w is a natural number not divisible by p. Denote $r=fp^i$. Since $f\mid r$, we get by Lemma 4 that $T_r(a)-1\equiv 0 \mod p$. Compute

$$\frac{T_n(a)-1}{T_r(a)-1}=\frac{T_w((T_r(a)-1)+1)-1}{T_r(a)-1}\equiv w^2 \mod p,$$

where the congruence is obtained by putting $n=w$ and $x=T_r(a)-1$ in Proposition 11. Suppose $w>1$. This implies $r<n$. Hence $\Omega_n(a)$ is a divisor of $\frac{T_n(a)-1}{T_r(a)-1}$ by Lemma 6. But $p\mid\Omega_n(a)$, so we get $p\mid w^2$, contrary to the definition of w. Thus $w=1$ and $n=fp^i$.

Suppose $i>0$. Lemma 5 asserts that f divides one of the numbers $p-1,p,p+1$, and that $(p,f)=(2,3)$ is not possible. Thus p is the greatest prime divisor of n.

Define $s=fp^{i-1}$. By Lemma 4 we have $T_s(a)-1\equiv 0 \mod p$. Assume $p\geq 5$. Compute

$$\frac{T_n(a)-1}{T_s(a)-1}=\frac{T_p((T_s(a)-1)+1)-1}{T_s(a)-1}\equiv p^2 \mod p^3,$$

where the congruence is obtained by putting $n=p$ and $x=T_s(a)-1$ in Proposition 11. Since $s\mid n$ and $s<n$ we get by Lemma 6 that $\Omega_n(a)^{\sigma_n}$ is a divisor of $\frac{T_n(a)-1}{T_s(a)-1}$. So if $p^2\mid\Omega_n(a)$ and $n\geq 3$ we get a contradiction with the above computation. Thus if $p^2\mid\Omega_n(a)$, then we have $p=2,3$ or $n=2$.

Consider first the case when $p=2$. Since p is the greatest prime divisor of n, we have $n=2^i$. So $4\mid\Omega_{2^i}(a)$. For $i>1$ we have $\Omega_{2^i}(a)=2T_{2^{i-2}}(a)$ (see Section 1.2. in [Riv] for the zeros of T_n). But $2T_{2^{i-2}}(a)\equiv 2 \mod 4$ for $i>2$ (for $i=3$ we have $2T_2(x)=4x^2-2$, and for higher i use the composition identity). Thus $i\in\{1,2\}$, so $n\in\{2,4\}$.

Now let $p=3$. Since p is the greatest prime divisor of n, we have $n=2^j3^i$ with $i\geq 1$.
Consider first the case when $j=0$. The only zero in $\mathbb{Z}/9\mathbb{Z}$ of the polynomial $\Omega_3(x)=2x+1$ is $x=4$. Computing the image of T_3 on $\mathbb{Z}/9\mathbb{Z}$ we get $\{0,1,8\}$. So by Proposition 7 we have that $9\mid\Omega_n(a)$ implies $n=3$.
Now consider the case when $j\geq 1$. The only zero in $\mathbb{Z}/9\mathbb{Z}$ of the polynomial $\Omega_6(x)=2x-1$ is $x=5$. Computing the image of T_2 on $\mathbb{Z}/9\mathbb{Z}$ we get $\{1,4,7,8\}$, and as we said above the image of T_3 is $\{0,1,8\}$. So by Proposition 7 we have that $9\mid\Omega_n(a)$ implies $n=6$.
Thus if $9\mid\Omega_n(a)$ then $n\in\{3,6\}$.

Now let $n=2$. We get that $f=1$ and $p=2$. □

Corollary 14. *Let $a,n>1$ be natural numbers. A prime number p such that $n=\mathrm{Che}_p(a)$ does not exists if and only if $\Omega_n(a)$ is either a power of an odd prime number that is the greatest prime divisor of n, or a power of 2.*

Proof. Suppose first that $\Omega_n(a)$ has at least 2 distinct prime divisors, p_1 and p_2. By Theorem 13 we have $n=\mathrm{Che}_{p_1}(a)p_1^{i_1}=\mathrm{Che}_{p_2}(a)p_2^{i_2}$. If neither $\mathrm{Che}_{p_1}(a)$ nor $\mathrm{Che}_{p_2}(a)$ equals n, then $i_1,i_2>0$. But this means that both p_1,p_2 are the greatest prime divisor of n. By the contradiction we have $\mathrm{Che}_{p_1}(a)=n$ or $\mathrm{Che}_{p_2}(a)=n$.

Now suppose that $\Omega_n(a)$ is a power of an odd prime number p coprime to n. By Theorem 13 we have $\mathrm{Che}_p(a)=n$.

Suppose that $\Omega_n(a)$ is a power of an odd prime number p dividing n. By Lemma 5 we have that Che_p is coprime to p. So by Theorem 13 we get that $n=\mathrm{Che}_p(a)p^i$ with $i>0$. Thus $n\neq\mathrm{Che}_p(a)$.

We also get that p is the greatest prime divisor of n.

Let $\Omega_n(a)$ be power of 2. By Lemma 5 the possible values of $\mathrm{Che}_2(a)$ are 1 or 2. Hence if $n = \mathrm{Che}_p(a)$ then $n = 2$. So $\Omega_2(a) = 2(a+1)$ is a power of 2. Thus a is odd and we have $\mathrm{Che}_2(a) = 1$.

□

Proof of Theorem 1. First we show that the exceptional cases described in Corollary 14 can appear for $n \in \{2, 3, 4, 6\}$ only.

Let $\Omega_n(a)$ be power of an odd prime number p that is the greatest prime divisor of n. Suppose $n \notin \{2, 3, 4, 6\}$. By Theorem 13 we get $\Omega_n(a) = p$. For $1 \le k \le \frac{n}{2}$ we have $a - \cos\frac{2k\pi}{n} > a - 1$. Since $p \mid n$, we get $p - 1 = \varphi(p) \mid \varphi(n)$. Hence

$$p = \Omega_n(a) = \prod_{\substack{1 \le k \le \frac{n}{2} \\ \gcd(k,n)=1}} 2(a - \cos\tfrac{2k\pi}{n}) > (2(a-1))^{\frac{\varphi(n)}{2}} \ge (2(a-1))^{\frac{p-1}{2}}.$$

This implies $a = 2$ and $p \in \{3, 5\}$. Suppose $p^2 \mid n$. This means that $p \mid \frac{n}{p}$. Thus by Proposition 7 we have $\Omega_n(x) = \Omega_{p\frac{n}{p}}(x) = \Omega_{\frac{n}{p}}(T_p(x))$. Using this, we get as above

$$p = \Omega_n(2) = \Omega_{\frac{n}{p}}(T_p(2)) > (2(T_p(2)-1))^{\frac{\varphi\left(\frac{n}{p}\right)}{2}} \ge (2(T_p(2)-1))^{\frac{p-1}{2}}.$$

But $T_3(2) - 1 = 25$ and $T_5(2) - 1 = 361$, a contradiction. Hence $n = p \cdot \mathrm{Che}_p(2)$. We have $\mathrm{Che}_3(2) = 2$ and $\mathrm{Che}_5(2) = 3$. So $n = 6$ or $n = 15$. But $\Omega_{15}(2) = 5 \cdot 29$, so it is not a power of 5. Thus $n = 6$, a contradiction.

Now let $\Omega_n(a)$ be a power of of 2. Suppose $n \notin \{2, 3, 4, 6\}$. By Lemma 5 and Theorem 13 we get that $n = 2^i$, $i \ge 3$, and $\Omega_n(a) = 2$. We use the identity $\Omega_{2^i} = 2T_{2^{i-2}}$. For $a \ge 2$ the sequence $T_n(a)$ is strictly increasing and $T_0(a) = 1$. Thus $\Omega_n(a) > 2$, a contradiction.

Hence the exceptional cases can appear only for $n \in \{2, 3, 4, 6\}$. We obtain the values of corresponding a by examining $\Omega_2(a) = 2(a+1)$, $\Omega_3(a) = 2a+1$, $\Omega_4(a) = 2a$, and $\Omega_6(a) = 2a-1$, according to Corollary 14. □

Acknowlegements

The Magma online calculator was more than helpful. We found the formulas for the coefficients in Proposition 11 thanks to OEIS database. We are grateful to Bartłomiej Bzdęga for suggestions regarding the proof of Proposition 9.

References

[Riv] Theodore. J. Rivlin, *Chebyshev Polynomials: From Approximation Theory to Algebra and Number Theory*, second edition, Wiley Interscience 1990.

[Lün1] Heinz Lüneburg, *Ein einfacher Beweis für den Satz von Zsigmondy über primitive Primteiler von $A^N - 1$*, Geometries and groups (Berlin, 1981), pp. 219-222, Lecture Notes in Math., 893, Springer, Berlin-New York, 1981.

[Lün2] Heinz Lüneburg, *Galoisfelder, Kreisteilungskörper und Schieberegisterfolgen*, Bibliographisches Institut, Mannheim, 1979.

Faculty of Mathematics and Computer Science, Adam Mickiewicz University, ul. Uniwersytetu Poznańskiego 4, 61-416 Poznań, Poland

E-mail address: stefbar@amu.edu.pl