T.C.

ULUDAĞ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSİTİTÜSÜ

$H(\lambda_q)$ HECKE GRUPLARI İLE İLGİLİ MİNİMAL POLİNOMLAR

Birsen ÖZGÜR

Prof. Dr. İsmail Naci CANGÜL

(Danışman)

DOKTORA TEZİ

MATEMATİK ANA BİLİM DALI

BURSA 2013

TEZ ONAYI

Birsen ÖZGÜR tarafından hazırlanan "$H(\lambda_q)$ Hecke Grupları ile İlgili Minimal Polinomlar" adlı tez çalışması aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Uludağ Üniversitesi Fen Bilimleri Enstitüsü Matematik Ana Bilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Danışman **:** Prof. Dr. İsmail Naci CANGÜL

Başkan : Prof. Dr. İsmail Naci CANGÜL İmza

Uludağ Üniversitesi, Fen-Edebiyat Fakültesi, Matematik Bölümü

Üye : Prof. Dr. Cevdet DEMİR İmza

Uludağ Üniversitesi, Fen-Edebiyat Fakültesi, Kimya Bölümü

Üye : Prof. Dr. Osman BİZİM İmza

Uludağ Üniversitesi, Fen-Edebiyat Fakültesi, Matematik Bölümü

Üye : Prof. Dr. Recep ŞAHİN İmza

Balıkesir Üniversitesi, Fen-Edebiyat Fakültesi, Matematik Bölümü

Üye : Doç. Dr. Basri ÇELİK İmza

Uludağ Üniversitesi, Fen-Edebiyat Fakültesi, Matematik Bölümü

Yukarıdaki sonucu onaylarım.

Prof. Dr. Kadri ARSLAN

Enstitü Müdürü

.. /.. / 2013

U. Ü. Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,

- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,

- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,

- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,

- kullanılan verilerde herhangi bir tahrifat yapmadığımı,

- ve bu tezin herhangi herhangi bir bölümünü bir üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı,

beyan ederim.

26 / 02 / 2013

İmza

Birsen ÖZGÜR

ÖZET

Doktora Tezi

$H(\lambda_q)$ HECKE GRUPLARI İLE İLGİLİ MİNİMAL POLİNOMLAR

Birsen ÖZGÜR

Uludağ Üniversitesi

Fen Bilimleri Enstitüsü

Matematik Anabilim Dalı

Danışman: Prof. Dr. İ. Naci CANGÜL

$H(\lambda_q)$ Hecke Grubu, $q \in \mathbb{N}$, $q \geq 3$ olmak üzere $\lambda_q = 2cos\,\pi/q$ için $R(z) := -\frac{1}{z}$ ve $T(z) := z + \lambda_q$ kesirli doğrusal dönüşümleri tarafından üretilen $PSL(2,\mathbb{R})$'nin ayrık bir alt grubudur. Hecke gruplarının denklik ve temel denklik alt gruplarının belirlenmesi hala açık bir problemdir. Modüler grup için bu alt grupların tümü belirlenmiştir. Hecke grupları için sadece seviyesi asal sayı olan denklik ve temel denklik alt gruplarının hesabı Cangül tarafından yapılmıştır, Cangül, 1993. Asal olmayan seviyeye sahip olan denklik ve temel denklik alt gruplarının hesaplanabilmesi için λ_q sayısının bu modlardaki değerlerinin hesaplanması gereklidir. Bu tez çalışmasında λ_q cebirsel sayısının matematiksel olarak anlamlı bir şekilde ifade edilemediği durumlarda bu sayının minimal polinomu olan P_q^* ile ilgili MAPLE kullanılarak hesaplamalar yapılmış ve $3 \leq q \leq 300$ için P_q^*'ın genişletilmiş bir listesi verilmiştir. Buna ek olarak çeşitli q değerleri için λ_q cebirsel sayısının minimal polinomlarının asal moddaki köklerine ilişkin ispatları ile birlikte çeşitli sonuçlar elde edilmiştir. Elde edilen bu sonuçlar, ayrık gruplar teorisinin önemli bir problemi olan Hecke gruplarının denklik alt gruplarının incelenmesinde oldukça yarar sağlayacaktır ve bundan sonraki çalışmalara da ışık tutacaktır. Web'de http://www.scribd.com/documents adresine koyduğumuz polinom listelerine gösterilen yoğun ilgi gelecekte de bu polinomların bir çok çalışmaya faydasının olacağının bir göstergesidir. Tezde P_q^* minimal polinomları dışında Hecke gruplarıyla ilgili çeşitli hesaplamaların yapılmasında kullanılacak bazı cebirsel sayı sınıflarının da minimal polinomları hesaplanmıştır.

Anahtar Kelimler: Minimal polinomlar, Chebycheff polinomları, Dickson polinomları, Hecke grupları, Temel denklik alt grubu

2013, ix + 157 sayfa.

ABSTRACT

MINIMAL POLYNOMIALS RELATED TO HECKE GROUPS $H(\lambda_q)$

Birsen OZGUR

Uludag University

Institute of Natural Sciences

Department of Mathematics

Supervisor: Prof. Dr. I. Naci CANGUL

The Hecke group $H(\lambda_q)$ is the discrete subgroup of $PSL(2,\mathbb{R})$ which is generated by two linear fractional transformations defined as $R(z) := -\frac{1}{z}$ and $T(z) := z + \lambda_q$ for $q \in \mathbb{N}$, $q \geq 3$, $\lambda_q = 2cos\,\pi/q$. It is an open problem to determine the congruence and principal congruence subgroups of the Hecke groups. For the modular groups case, all these subgroups are determined. In Cangul 1993, Cangul determined the congruence and principal congruence subgroups of prime level of the Hecke groups. To find those subgroups having non-prime level, it is necessary to reduce the values of λ_q in these modules. In this thesis, some calculations related to the minimal polynomials P_q^* of algebraic number λ_q, when this number cannot be properly reduced have been done by means of MAPLE and the extended lists of P_q^* have been given for $3 \leq q \leq 300$. In additon to these proofs with some corollaries concerning the roots of minimal polynomials of algebraic number λ_q in modulo prime $\wp$ have been obtained for various values of q. These corollaries have been very useful in investigation of congruence subgroups of Hecke groups which is both main subject of this thesis and an important open problem in discrete group theory. Also these corollaries will be a guide for the future works. The attention shown to the lists of polynomials that we put to the web address http://www.scribd.com/documents clearly shows that these polynomials are going to be useful to many researchers in the future. In this thesis, some minimal polynomials apart from P_q^* of some algebraic numbers which are useful in several studies related to Hecke groups have also been calculated.

Key Words: Minimal polynomial, Chebycheff polynomials, Dickson polynomials, Hecke groups, principal congruence subgroups

2013, ix + 157 pages.

TEŞEKKÜR

"İnanmak, başarmanın yarısıdır" sözü doktoranın hatta hayatta bir işi başarabilmenin temel inanç felsefelerinden biridir. Doktoraya başladığım ilk gün "senin bu işi başaracağına inanıyorum" sözleri ile öncelikle bana bu inancı ve özgüveni aşılayan daha sonra da bütün bu süre boyunca beni yönlendiren yolumu aydınlatan bu zorlu süreci kolaylaştıran bu seviyeye gelebilmem için elinden geldiğince beni yetiştirmeye çalışan çok değerli hocam ve danışmanım Prof. Dr. İsmail Naci CANGÜL'e saygılarımı sunar, canı gönülden teşekkür ederim.

Doktora süresi boyunca özellikle de tez çalışmaları döneminde bana her anlamda destek olan başta anne ve babam olmak üzere ailemin her bir üyesine ayrı ayrı teşekkürlerimi sunarım.

Son olarak da doktoramın bitmesi için bana dua eden yakın akrabalarıma ve sevgili arkadaşlarıma da teşekkürü bir borç bilirim.

Birsen ÖZGÜR

26 /02/ 2013

İÇİNDEKİLER

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler	Açıklamalar
$H(\lambda_q)$	Hecke grubu
$\mathbb{Z}$	Tam sayılar halkası
$\mathbb{R}$	Reel sayılar cismi
$\mathbb{C}$	Kompleks sayılar cismi
$\mathbb{Q}$	Rasyonel sayılar cismi
F, K, E	Cisim
$F[x]$	F cismi üzerindeki polinomlar halkası
$F(u)$	F cisminin u ile basit genişlemesi
ζ_n	Birimin n. ilkel kökü
$G(K/F)$	K cisminin F cismi üzerindeki galois grubu
φ	Euler fonksiyonu
$GF(q)$	q elemanlı galois cismi
$\mathcal{U}$	Üst yarı düzlem
Γ	Fuchs grubu
$(g;\ m_1, \dots, m_r; t; u)$	Fuchs grubunun gösterimi
Γ^*	Hiperbolik üçgenin yansımaları tarafından üretilen grup
(l, m, n)	Hiperbolik üçgen grubu
μ	İndeks
n	Seviye
t	Parabolik sınıf sayısı
N	Normal alt grup
G	Herhangi bir grup
g	Bir serbest grubun cinsi
λ	Sabit pozitif bir reel sayı

q	$q \geq 3$ koşulunu sağlayan bir tamsayı
F_λ	$H(\lambda)$ grubu için bir temel bölge
$H(\lambda_3)$	Modüler grup
$H(\sqrt{m})$	${\lambda_q}^2 = m$ için hecke grubu
$R(z), T(z), S(z)$	Kesirli doğrusal dönüşümler
R, S	Eliptik üreteçler
T	Parabolik üreteç
ψ_n	$\mathbb{Q}$ üzerinde $cos\ 2\pi/n$'nin minimal polinomu
T_n	n-inci Chebycheff polinomu
D_n	n-inci Dickson polinomu
$\mathbb{Q}(\zeta_n)$	$\mathbb{Q}$ cisminin ζ_n ile genişlemesi
P_q^*	$\mathbb{Q}$ üzerinde $\lambda_q = 2cos\,(\pi/q)$'nun minimal polinomu
deg P_q^*	P_q^* minimal polinomunun derecesi
$\Gamma(n)$	Γ'nın n seviyeli temel denklik alt grubu
$\Gamma_p(\sqrt{m})$	$H(\sqrt{m})$'nin p seviyeli temel denklik alt grubu
$\Gamma_p(\lambda_q)$	$H(\lambda_q)$'nun p seviyeli temel denklik alt grubu
$\mathbb{Z}[\lambda_q]$	Tam sayılar halkasının λ_q ile genişlemesi
$\wp$	$\mathbb{Z}[\lambda_q]$'nun bir ideali
u	$GF(p^s)$'de $P_q^*(\lambda_q)$'nin bir çözümü
$\Theta_{p,u,q}$	$\lambda_q \mapsto u$ dönüşümü tarafından indirgenen homomorfizm
$K_{p,u}(\lambda_q)$	$H(\lambda_q)$'nun p seviyeli normal bir denklik alt grubu ya da $\Theta_{p,u,q}$ dönüşümünün çekirdeği
$K_{p,u}(\sqrt{m})$	$H(\sqrt{m})$'nin p seviyeli denklik alt grubu
ψ	Halka homomorfizması
$\overline{\psi}$, $\underline{\psi}$	Grup homomorfizması
$\mathbb{Z}_p[\lambda_q]$	$\mathbb{Z}[\lambda_q]$'nun p asal modundaki halka genişlemesi

φ_p	$\mathbb{Z}[\lambda_q]$'nun tüm elemanlarını p modunda indirgeyen halka homomorfizması
χ_u	$P_q^*(\lambda_q)$'nun her bir u kökü için λ_q'yu u'ya götüren halka homomorfizması
R_p, S_p, T_p	p modundaki üreteçler
$H_p(\lambda_q)$	R_p, S_p tarafından üreteilen p modundaki $H(\lambda_q)$ grubu
$\underline{\varphi_p}, \underline{\chi_u}$	Grup homomorfizması
$SL(2, K)$	Özel lineer grup
$PSL(2, K)$	Projektif özel lineer grup
$(C_3 \times C_3) \wr C_2$	$C_3 \times C_3$ ile C_2' nin wreath çarpımı

ŞEKİLLER DİZİNİ

Sayfa

1. GİRİŞ

TEMEL BİLGİLER

Bu bölümde, bu tez çalışmasına ışık tutacak bir takım temel bilgilere yer verilecektir. Bu bilgiler arasında cisim genişlemeleri ve Galois cisimleri, Fuchs grupları, $H(\lambda_q)$ Hecke gruplarını hatırlamak oldukça yararlı olacaktır. Bu kısımdaki temel bilgilerin hazırlanmasında Cangul (1993) doktora tezi, Fraleigh (1974), Fraleigh (2002), Grillet (2007) ve Kurur (2007) kaynaklarından yararlanılmıştır.

1.1. Cisim Genişlemeleri

Sonlu cisim genişlemeleri, bu tez çalışmasında ihtiyaç duyulacak bilgiler arasındadır. Pek çok cisim genişlemeleri mevcuttur fakat giriş kısmının bu bölümünde daha çok basit genişlemeler üzerinde durulacaktır.

Tanım 1.1.1. K bir cisim olsun. Eğer K cismini kapsayan bir E cismi varsa yani $K \subseteq E$ olacak şekilde varsa E'ye K'nın bir **cisim genişlemesi** denir.

Tanım 1.1.2. K bir cisim**,** V bir vektör uzayı olsun. V'yi üreten doğrusal (lineer) bağımsız kümeye V vektör uzayının K cismi üzerindeki bir **tabanı** adı verilir.

Tanım 1.1.3. V bir vektör uzayı olsun. V'nin herhangi bir tabanındaki eleman sayısına bu vektör uzayının **boyutu** adı verilir.

Bir K cismi üzerindeki $K[X]$ polinomlar halkası, bir vektör uzayıdır ve $K[X]$ vektör uzayının boyutu sonsuzdur, bu vektör uzayının tabanı olarak $\{1, X, X^2, \ ...\}$ seçilebilir. Her bir $p \in K[X]$ polinomuna karşılık gelen bir bileşen vardır. Örneğin $p(X) = 3 + X + 3X^3$ polinomuna $(3, 1, 0, 3, 0, 0, 0, \ ...)$ bileşeni karşılık gelir.

Örnek 1.1.4. $\mathbb{C}$'nin, $\mathbb{R}$ üzerindeki bir tabanı $\{1, i\}$ olsun. O zaman her $a + bi$ elemanı $a(1) + b(i)$ olarak ifade edilebilir. Dolayısıyla $a + bi$ elemanı, (a, b) bileşeni olarak da temsil edilebilir.

E, K cisminin bir genişlemesi olsun. Yani E, K cisim ve $K \subseteq E$ olsun. Her $a, b \in K$ ve $a, b \in E$ için $a(u + v) = au + av$ ve $(a + b)u = au + bu$ vektör uzayı olma koşulları sağlandığından E, K cismi üzerinde bir vektör uzayı olarak düşünülebilir.

Örneğin $\mathbb{C}$, $\mathbb{R}$'yi kapsayan bir cisimdir. Dolayısı ile $\mathbb{C}$, $\mathbb{R}$ üzerinde bir vektör uzayıdır. Diğer bir örnek de $\mathbb{Q}[\sqrt{2}] = \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \}$, $\mathbb{Q}$'yu kapsayan bir cisimdir ve $\mathbb{Q}$ üzerinde bir vektör uzayıdır.

Tanım 1.1.5. E, K cisminin bir genişlemesi yani $K \subseteq E$ olsun. K üzerindeki E vektör uzayının boyutuna, K cisminin E cismine genişlemesinin **derecesi** adı verilir. $[E : K]$ ile gösterilir. Derece sonlu ise K cisminin E cismine genişlemesi de sonludur.

Tanım 1.1.6. E, K cisminin bir genişlemesi olsun. $\alpha \in E$ için α'yı K'ya katmakla elde edilen cisim $K(\alpha) = E$ olduğunda bu genişlemeye **basit genişleme** adı verilir.

$\mathbb{R}$'ye $i \in \mathbb{C}$ elemanının eklenmesiyle oluşan cisim, $\mathbb{C} = \mathbb{R}(\mathrm{i})$'dir. $\alpha = i$ için $\alpha^2 + 1 = 0$ olup α, $X^2 + 1$ polinomunun bir köküdür ve $\mathbb{R}$'de derecesi 2 olan bir genişlemeye sahiptir. yani $[\mathbb{C} : \mathbb{R}] = 2$ dir. Benzer şekilde $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ olduğu da görülebilir.

$\mathbb{Q}(\alpha)$'daki bir α elemanı için $a_k\alpha^k + \cdots + a_1\alpha + 1 = 0$ eşitliği olup α, $a_kX^k + \cdots + a_1X \quad + 1 = 0$ polinomunun bir köküdür. Böylece $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ genişlemesinin derecesi, α'nın kök olduğu en küçük dereceli polinomun derecesidir.

Örnek 1.1.7. $\mathbb{Q}[\sqrt[3]{2}] = \{ a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b. c \in \mathbb{Q} \}$'daki $\alpha = \sqrt[3]{2}$ için $\alpha^3 - 2 = 0$ olup $\alpha = \sqrt[3]{2}$, $X^3 - 2$ polinomunun bir köküdür ve $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$'tür.

Tanım 1.1.8. E, K cisminin bir genişlemesi olsun. Herhangi $\alpha \in E$ için α'yı kök kabul eden K üzerindeki en küçük dereceli birim başkatsayılı (monic) polinoma K üzerinde α'nın **minimal polinomu** denir.

Tanım 1.1.9. E, K cisminin bir genişlemesi olsun. Bir $\alpha \in E$ için $f(\alpha) = 0$ olacak şekilde sıfırdan farklı bir $f(x) \in K[X]$ varsa α'ya K üzerinde **cebirsel** denir.

Tanım 1.1.9.'a denk olarak şu söylenebilir: α'nın K üzerinde cebirsel olması için gerekli ve yeterli koşul $[E : K]$'nın sonlu olmasıdır. Örneğin $[\mathbb{C} : \mathbb{R}] = 2$ sonlu olduğunda

$\mathbb{C}$'nin her elemanı $\mathbb{R}$ üzerinde cebirseldir. $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$ sonlu olduğundan $\sqrt[3]{2} \in \mathbb{R}$, $\mathbb{Q}$'da cebirseldir.

Tanım 1.1.10. F bir cisim ve f, $F[x]$'de n dereceli indirgenemeyen birim başkatsayılı (monic) bir polinom olsun. u, f'nin bir kökü olacak biçimde Fye u'yu katmakla elde edilen $F(u)$ cismine F'nin bir $\boldsymbol{F(u)}$ **basit genişlemesi** denilir.

Tanım 1.1.11. $i = 0,1,\dots,n-1$ için $a_i \in F$ olmak üzere $F(u)$'nun her v elemanı

$$v = a_0 + a_1 u + \cdots + a_{n-1} u^{n-1}$$

olacak biçimde tek türlü temsil edilebiliyor ise v'ye $\boldsymbol{F}$ **üzerinde** $\boldsymbol{n}$**. dereceden cebirseldir** denilir.

Aşağıdaki teorem bir cismin basit bir genişlemesinin var olduğunu göstermektedir.

Teorem 1.1.12. F bir cisim ve f, $F[x]$'de n. dereceden indirgenemeyen birim başkatsayılı bir polinom olsun. O zaman f, minimal polinom ve u, F üzerinde cebirsel olacak biçimde F'nin bir $F(u)$ basit genişlemesi mevcuttur.

İspat. Teoremin ayrıntılı ispatı için Fraleigh (1974)'e bakınız.

Aşağıdaki tanım ve sonuçlar Euler fonksiyonu ile ilgilidir. Bu fonksiyona ait bilgiler minimal polinomların hesaplanmasında kullanılacaktır.

Tanım 1.1.13. $m \in \mathbb{Z}^+$, $0 \leq n \leq m-1$ olmak üzere $(m,n) = 1$ olacak şekildeki m tam sayılarının sayısına eşit olan fonksiyona **Euler fonksiyonu** denir ve bu fonksiyon φ ile gösterilir.

$n = 1$ için $\varphi(n) = 1$ olduğu açıktır. Bundan başka p asal olmak üzere $k \geq 1$, $n = p^k$ için $\varphi(n) = \varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$ ve özel olarak $\varphi(p) = p - 1$'dir.

Teorem 1.1.14. $m, n \in \mathbb{Z}^+$ için $(m,n) = 1$ ise

$$\varphi(mn) = \varphi(m)\varphi(n)$$

dir.

İspat. Kanıt için Jones (2005)'e bakınız.

Bu tez çalışmasında basit genişlemelerin önemli uygulamalarından biri olan döngüsel genişlemelere yer verilecektir.

Tanım 1.1.15. n. dereceden

$$\zeta^n - 1 = 0$$

döngüsel (cyclotomic) denkleminin bir kökü olan **birimin n. ilkel kökü** ζ ise $\mathbb{Q}$ rasyonel sayılar cismine ζ'nın eklenmesiyle elde edilen cisme **$\mathbb{Q}$'nun n'inci döngüsel (cyclotomic) genişlemesi** denir.

Aşağıdaki tanımlar ve sonuçlar, Galois Teori'ye ait temel bilgilerdir. Bunlar, minimal polinomun derecesinin belirlenmesinde yol gösterecektir.

Tanım 1.1.16. F, bir K cisminin alt cismi ve $u, v \in K$, F üzerinde cebirsel olsun. Eğer u ve v, F üzerinde aynı minimal polinoma sahip ise u ve v'ye F üzerinde **eşleniktir** denilir.

Tanım 1.1.17. $F \subseteq K \subseteq L$ olduğunda $u \in K$ ve F üzerinde u 'nun eşleniği $v \in L$ olduğunda $v \in K$ oluyorsa o zaman F üzerinde K'nın cisim genişlemesine **eşleniklik altında kapalıdır** denilir.

Teorem 1.1.18. K'nın eşleniklik altında kapalı olması için gerek ve yeter koşul f, K'da herhangi bir köke sahip $F[x]$'de indirgenemeyen bir polinom olduğunda f'nin K'da parçalanmasıdır. (Fraleigh 1974)

Tanım 1.1.19. K, F'nin bir genişlemesi olmak üzere eğer K eşleniklik altında kapalı ise K'ya F'nin bir normal genişlemesi denilir.

Tanım 1.1.20. K'nın F'yi sabit bırakan tüm otomorfizmalarının grubu $G(K/F)$ olmak üzere eğer K, F'nin sonlu bir normal genişlemesi ise $G(K/F)$'ye K'nın F üzerindeki **Galois Grubu** denilir.

Aşağıdaki teorem, Galois grubuna ait olan sonuçlardan biridir.

Teorem 1.1.21. $\mathbb{Q}$'nun n. döngüsel genişlemesinin Galois grubu $\varphi(n)$ elemanlıdır ve n modundaki birimlerin grubuna izomorftur.

İspat: Detaylı bir ispat için Fraleigh (1974)'te sayfa 472'ye bakınız.

Sonuç 1.1.22. Bir p asalı için $\mathbb{Q}$'nun n. döngüsel genişlemesinin Galois grubunun mertebesi $p-1$'dir.

1.2. Fuchs Grupları

Aşağıda Fuchs Grupları tanımlanmış ve bununla ilgili bilgiler verilmiştir.

Tanım 1.2.1. $\mathcal{U}$ üst yarı düzleminin konform dönüşümlerinin grubu olan $PSL(2,\mathbb{R})$'nin sonlu üreteçli ayrık alt gruplarına **Fuchs grubu** adı verilir.

Her bir Γ Fuchs grubu,

üreteçler: $a_1, b_1, \dots, a_g, b_g$ (hiperbolik dönüşümler),

$x_1, \dots, x_r$ (eliptik dönüşümler),

$p_1, \dots, p_t$ (parabolik dönüşümler),

$h_1, \dots, h_u$ (hiperbolik sınır dönüşümleri)

ve

bağıntılar: $x_j^{m_j} = \prod_{i=1}^{g}[a_i, b_i] \prod_{j=1}^{r} x_j \prod_{k=1}^{t} p_k \prod_{l=1}^{u} h_l = 1$, ($m_{\mathbf{1}}, \dots, m_r \geq 2$ tamsayıları Γ nın periyotları) olmak üzere

$$(g;\ m_1, \dots, m_r; t; u) \qquad (1.1)$$

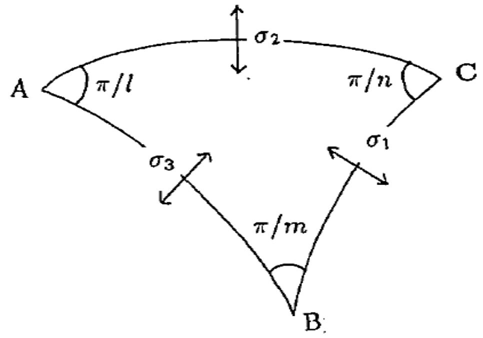
biçiminde bir gösterime sahiptir. Hecke gruplarının sonlu indeksli tüm normal alt grupları için $u = 0$ olduğundan Hecke grupları, hiperbolik sınır elemanına sahip değildir.

$H(\lambda_q)$ Hecke grupları, parabolik üreteçli üçgensel gruplar olarak düşünülebilir. Üçgensel grupların tanımı aşağıda verilmiştir:

$l, m, n \geq 2$ tamsayılar olmak üzere açıları $\pi/l, \pi/\mathrm{m}, \pi/n$ olan hiperbolik üçgeni dikkate alalım. Aşağıda şekil 1.1.'de gösterildiği gibi $\sigma_1, \sigma_2, \sigma_3$ bu üçgenin kenarları üzerindeki yansımalar olsun. Γ^* da bu yansımalar ile üretilen ve

$$\Gamma^* = \langle \sigma_1, \sigma_2, \sigma_3 \mid \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = (\sigma_2\sigma_3)^l = (\sigma_3\sigma_1)^m = (\sigma_1\sigma_2)^n = 1 \rangle$$

gösterimine sahip bir grup olsun.

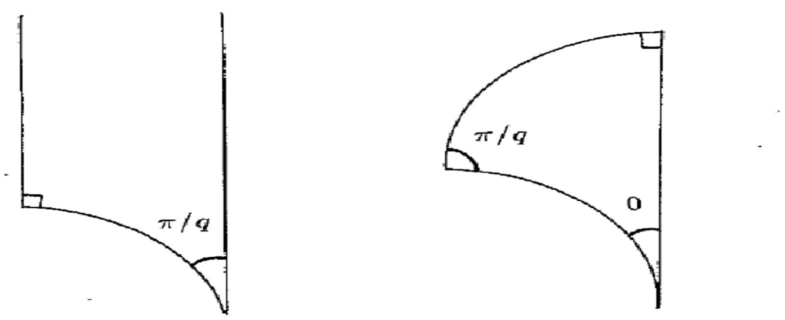


Şekil 1.1. Bir hiperbolik üçgenin yansımaları

$x = \sigma_2\sigma_3$ ve $y = \sigma_3\sigma_1$ olarak alınırsa x, A köşesinde π/l açısı kadar bir dönme ve y, B köşesinde π/m açısı kadar bir dönme dönüşümü olur. Bu durumda xy ise C köşesinde π/n açısı kadar bir dönmedir. Böylece Γ^*'ın sadece yön koruyan izometrilerini içeren

$$\Gamma = \langle x, y \mid x^l = y^m = (xy)^n = 1 \rangle$$

şeklinde gösterime sahip bir Γ alt grubu elde edilir. Bu grup, daha önce bir Fuchs grubunun gösterimine benzer şekilde $(0; l, m, n)$ gösterimi ile ifade edilebilir ve genellikle kısaca (l, m, n) olarak gösterilir. Bu gruba **üçgensel grup** adı verilir. Bu grubun Γ^* daki indeksi iki olduğundan Γ^*'ın bir normal alt grubudur.



Şekil 1.2. Hecke gruplarına karşılık gelen hiperbolik üçgenler

$H(\lambda_q)$ Hecke Grubu, $(0; 2, q, \infty)$ gösterimine sahip bir üçgensel gruptur. Ayrıca parabolik elemanların, sonsuz mertebeli eliptik elemanlar olduğu bilindiğinden $(xy)^\infty = 1$ olur. Böylece $H(\lambda_q)$, mertebesi 2 ve q olan iki sonlu devirli grubun serbest çarpımına izomorf olup

$$H(\lambda_q) \cong (2, q, \infty) \cong \langle x, y \mid x^2 = y^q = 1 \rangle$$

şeklinde bir üçgensel gruptur. Şekil 1.1'deki üçgenin $\pi/2, \pi/q, \pi/\infty = 0$ açılı Şekil 1.2.'deki üçgenlerden birine dönüştüğü kolayca görülebilir.

Aşağıda verilecek olan tanımlar μ indeks, n seviye ve t parabolik sınıf sayısı ile ilgilidir.

Tanım 1.2.2. N, $H(\lambda_q)$'nun μ indeksli bir normal alt grubu olsun. Maksimal parabolik devirli alt gruplarının eşlenik sınıflarının sayısına N'nin **parabolik sınıf sayısı** denir ve genellikle t ile gösterilir.

Tanım 1.2.3. N, $H(\lambda_q)$'nun μ indeksli bir normal alt grubu olsun. $T^n \in N$ özeliğindeki en küçük n pozitif tam sayısına N'nin **seviyesi** denir.

$$\mu = n.t$$

eşitliği indeks, seviye ve parabolik sınıf sayısı arasındaki ilişkiyi göstermektedir.

1.3. Hecke Grupları ve Modüler Grup

Bu bölümde Hecke grupları ve bunların en iyi bilineni olan modüler grupla ilgili bir takım bilgiler verilecektir. Daha sonra da bu bilgileri aydınlatıcı $H(\lambda_q)$ grubuna ilişkin bazı temel sonuçlara değinilecektir.

Hecke (1936) çalışmasında λ sabit pozitif bir reel sayı olmak üzere

$$R(z) := -\frac{1}{z} \quad \text{ve} \quad T(z) := z + \lambda$$

kesirli doğrusal (lineer) dönüşümleri tarafından üretilen $H(\lambda)$ gruplarını tanımlamıştır.

R ve T dönüşümleri matrisler yardımıyla

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{ve} \quad \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

olarak gösterilirler. $S = RT$ olsun.

$H(\lambda)$ süreksiz yani bir Fuchs grubu olduğunda bu grupların, Dirichlet serilerinin çalışılmasında oldukça yararlı olduğu bilinmektedir. Hecke (1936) çalışmasında $\lambda \geq 2$ bir reel sayı olması durumunda veya $\lambda < 2$ iken $q \geq 3$ bir tamsayı olmak üzere

$$\lambda = \lambda_q = 2cos\frac{\pi}{q}$$

olması durumunda

$$F_\lambda = \{\, z \in \mathcal{U} : |\, Re\, z\,| \; < \; \lambda/2, |\, z\,| > \lambda \,\}$$

kümesinin $H(\lambda)$ grubu için bir temel bölge olduğunu ve diğer $\lambda > 0$ durumları için de bu kümenin temel bölge olmadığını göstermiştir. Buradan da $H(\lambda)$'nın bir Fuchs grubu olması için gerek ve yeter şartın $\lambda = \lambda_q$ veya $\lambda \geq 2$ bir reel sayı olması gerektiği görülür. Her iki durumda da $H(\lambda)$ grubuna **Hecke grubu** adı verilir. Bu tez çalışmasında $\lambda < 2$ durumu ile ilgilenilecek ve λ_q'ya karşılık gelen grup $H(\lambda_q)$ ile gösterilecektir. O halde $H(\lambda_q)$, $T(z) \coloneqq z + \lambda_q$ olmak üzere R ve T tarafından üretilen $PSL(2,\mathbb{R})$'nin ayrık bir alt grubudur.

En önemli ve en çok çalışılan Hecke grubu, $q = 3$ durumunda elde edilen $H(\lambda_3)$ modüler grubudur. Modüler grup durumunda $\lambda_3 = 2cos\frac{\pi}{3} = 1$'dir. Böylece bu grup için cisim genişlemesi $\mathbb{Q}(1) = \mathbb{Q}$ olarak bulunur. Yani $H(\lambda_3)$ 'ün elemanlarının katsayılarının tümü birer rasyonel tamsayıdır.

Literatürde modüler grubu temsil etmek için Γ veya $\Gamma(1)$ sembolleri kullanılır. Bu çalışmada daha çok Γ veya $H(\lambda_3)$ sembolleri kullanılacaktır.

Sadece modüler grup için doğru olup diğer Hecke grupları için doğru olmayan bazı sonuçlar vardır. Bunun temel sebebi $q > 3$ için $\mathbb{Q}(\lambda_q)$ cisim genişlemesinin açık olarak $\mathbb{Q}$'dan hatta $\mathbb{Q}$'nun basit bir genişlemesinden çok daha karmaşık olmasıdır. Bundan dolayı $q > 3$ için $H(\lambda_q)$'nun elemanlarının katsayıları, Γ'nın elemanlarının katsayıları olan tamsayılardan çok daha karmaşıktır. Bunun doğal bir sonucu olarak da yapılan tüm hesaplamalar, modüler grup durumda yapılan hesaplamalardan çok daha karışıktır.

$q = 4$ ve 6 için elde edilen $H(\lambda_q)$ Hecke grupları, modüler gruptan sonraki en önemli iki gruptur. Bu durumda sırasıyla $\lambda_q = \sqrt{2}$ ve $\sqrt{3}$ 'tür. Bundan dolayı da bu iki grubun cisim genişlemeleri, $\mathbb{Q}$ rasyonel sayılar cisminin ikinci dereceden (quadratic) genişlemeleri olan $\mathbb{Q}(\sqrt{2})$ ve $\mathbb{Q}(\sqrt{3})$'tür.

$q = 5$ için elde edilen $H(\lambda_5)$, diğer önemli Hecke gruplarından biridir. Bu durumda bu grubun cisim genişlemesi yine $\mathbb{Q}$'nun ikinci dereceden bir genişlemesi olur.

$q = 3, 4,$ 5 ve 6 için elde edilen $H(\lambda_q)$ Hecke grupları, λ_q değerinin, derecesi üçten küçük olan bir polinomun kökü olduğu halde elde edilen gruplardır.

$q \in \mathbb{N}$, $q \geq 7$ olduğunda λ_q, derecesi üç veya üçten büyük olan bir polinomun bir köküdür. Bunun sonucu olarak ilk dört durumda olduğu gibi λ_q sayısı, açıkça kolay bir şekilde belirlenemeyecektir. Bunun için $\mathbb{Q}$ üzerinde λ_q 'nun minimal polinomu belirlenmeye çalışılacaktır. Bu da tezin ilerleyen bölümlerinde q'nun tek ve çift olduğu durumlar için ayrı ayrı minimal polinomların belirlenip bunların hangi durumlarda ne tür bir köke sahip olduğunun incelenmesine yol açacaktır.

Modüler gruptan sonraki en önemli iki Hecke grubunun $\mathrm{H}(\sqrt{2})$ ve $\mathrm{H}(\sqrt{3})$ olmasının sebeplerinden biri, elemanları tam olarak bilinen tek Hecke gruplarının bunlar olmasıdır. $m = 2$ veya 3 için $H(\sqrt{m})$ grubu aşağıda belirtilen (i) ve (ii) biçimindeki matrislere karşılık gelen dönüşümlerden oluşmaktadır:

$$\text{(i)} \begin{pmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{pmatrix} \qquad a, b, c, d \in \mathbb{Z}, \quad ad - mbc = 1$$

$$\text{(ii)} \begin{pmatrix} a\sqrt{m} & b \\ c & d\sqrt{m} \end{pmatrix} \qquad a, b, c, d \in \mathbb{Z}, \quad mad - bc = 1 \tag{1.2}$$

(i) türündeki matrislere **çift elemanlar,** (ii) türündeki matrislere **tek elemanlar** adı verilir.

(1.2)'deki elemanların çarpımı, aynen pozitif ve negatif sayıların çarpımına benzerdir. Yani

tek.tek = çift.çift = çift,   çift.tek = tek.çift = tek

eşitlikleri geçerlidir.

1.4. $H(\lambda_q)$'nun Temel Denklik Alt Grupları

1.4.1. $H(\lambda_q)$'nun temel denklik alt gruplarının elde edilişi

Bu tezin amacı, $q \in \mathbb{N}$ ve $q \geq 3$ olmak üzere $\lambda_q = 2cos\,\pi/q$ cebirsel sayısına karşılık gelen $H(\lambda_q)$ Hecke grupları ve bu grupların alt gruplarının çalışılmasında karşılaşılan bazı trigonometrik sayıların minimal polinomlarıyla ilgili bazı teorik sonuçların elde edilmesinin yanı sıra MAPLE ile bu minimal polinomların listelerinin elde edilmesine yarayacak program rutinlerinin yazılmasıdır.

Önceki bölümde bazı küçük q değerleri ($q = 3, 4, 5$ ve 6) için $\lambda_q = 2cos\,\pi/q$ cebirsel sayısının işe yarar bir şekilde ifade edilebilmesinin sağladığı avantajlardan kısaca bahsedildi. Bu avantajlardan birisi Hecke gruplarının denklik ve temel denklik alt gruplarının hesaplanmasında ortaya çıkmaktadır. Aşağıda detaylı bir şekilde anlatılacağı gibi n seviyeli bir denklik ya da temel denklik alt grubunun hesaplanabilmesi için $H(\lambda_q)$ Hecke grubundaki tüm elemanların bir homomorfizma altındaki resimlerinin bulunması gereklidir. Bu homomorfizma elemanları n modunda indirgeyen homomorfizmadır.

$q = 3, 4, 5$ ve q'nun çeşitli değerleri için de $H(\lambda_q)$'nun temel denklik alt grupları Cangül (1993) tarafından verilmiştir. Bu tezin başlangıç amacı, Cangül (1993)'ün çalışması göz önünde bulundurularak $H(\lambda_q)$'nun temel denklik alt gruplarının elde edilmeye çalışılmasıydı. Ancak açık bir problem olan bu sorunun tam çözümüne yönelik çabalar sahip olunan süre içinde problemin tamamıyla çözülmesine yetmemiştir.

Doktora sonrası çalışmalarda bu problemin tam çözümü, olmazsa da kısmi çözümüne yönelik çalışmalar yapılması planlanmaktadır.

Şimdi yukarıda bahsedilen indirgeme homomorfizmasına dönelim.

Doğal olarak λ_q cebirsel sayısı $q = 3$ durumu dışında bir tamsayı olmadığından $q > 3$ durumlarında bu sayıyı tamsayı olarak düşünebilir miyiz sorusu akla gelmektedir. Bu da belli modlarda mümkündür. Yani belirli $\mathbb{Z}_n$ halkaları üzerinde λ_q sayısını bir tamsayı olarak düşünebiliriz.

Burada ilk sorun Hecke gruplarının elemanlarının yapısının bilinmesidir. İlk dört Hecke grubu için tüm elemanların yapısı belirli sınıflara ayrılarak literatürde yer almıştır. $q = 3$ durumunda zaten tüm elemanlar $(az + b)/(cz + d)$ şeklindeki tamsayı katsayılı dönüşümlerdir ve burada a, b, c ve d katsayılarının n modunda indirgenmesi kavramı zaten bilinen indirgeme kavramıdır. $q = 4$ ve 6 olması durumlarında elemanlar tek ve çift elemanlar olarak iki sınıfa ayrılmıştır. Bu iki durumda elamanların katsayılarının $\sqrt{2}$ ve $\sqrt{3}$ sayılarına bağlı olması nedeniyle katsayıların tamsayı olarak düşünülebilmesi ancak $\sqrt{2}$ ve $\sqrt{3}$ sayılarının tamsayı olarak düşünülebildiği durumlarda mümkündür. Bu da asal sayı modlarında 2 ve 3 sayılarının ikinci dereceden kalan olmalarıyla mümkündür. Son olarak $q = 5$ durumunda tüm grup elemanlarının sınıflandırılması $q = 4$ ve 6 olması durumlarındaki kadar net olmasa da lineer kesirler yardımıyla yapılmıştır. Burada da cebirsel sayı olarak λ_5 sayısının ikinci dereceden bir sayı olması nedeniyle ikinci dereceden kalanlar yardımıyla denklik ve temel denklik alt gruplarının hesaplanması mümkün olabilmektedir.

Ancak $q > 6$ durumunda λ_q sayısının en az üçüncü dereceden bir cebirsel sayı olması nedeniyle ne bildiğimiz indirgemeden ne de ikinci dereceden kalanlardan faydalanmamız mümkün değildir. $q = 7$ ve 9 durumlarında kübik rezidülerden faydalanabilmek sözkonusu olsa da genel olarak λ_q sayısının bir tamsayı olarak da düşünülebileceği modları hesaplamak zordur. Bu nedenle λ_q sayısının $\mathbb{Q}$ rasyonel sayılar cismi üzerindeki minimal polinomunun belli modlarda çalışılmasına ihtiyaç duyulmaktadır. Yani λ_q sayısını bir tamsayı olarak düşünemediğimiz durumlarda verilen modda minimal polinomu düzenleyerek köklerini bulup λ_q sayısının o moddaki (varsa) tamsayı değerini elde etmek mümkün olmaktadır.

$H(\lambda_q)$ Hecke grupları, hatırlanacağı gibi T parobolik elemanlı üçgensel gruplardır. $T^n \in N$ özelliğini sağlayan en küçük n pozitif tam sayısı, $H(\lambda_q)$'nun bir N alt grubunun seviyesidir. $\mu = |H(\lambda_q) : N|$ ve t, N'nin parabolik sınıf sayısını göstermek üzere $\mu = n.t$ bağıntısı geçerlidir.

Aşağıda ilk olarak modüler grubun denklik alt gruplarına ilişkin bilgiler verilmektedir.

Tanım 1.4.1.1. $n \in \mathbb{Z}^{+}$ olmak üzere, ***Γ*'nın *n* seviyeli temel denklik alt grubu**

$$\Gamma(n) = \left\{T(z) = \frac{az+b}{cz+d} \in \Gamma : a \equiv d \equiv \mp 1,\ b \equiv c \equiv 0\ (mod\ n)\right\}$$

olarak tanımlanır.

Tanım 1.4.1.2. Γ'nın $\Gamma(n)$ temel denklik alt grubunu içeren bir alt grubuna ***Γ*'nın *n* seviyeli denklik alt grubu** adı verilir.

Γ modüler grubunun normal denklik alt gruplarının tam bir sınıflandırılması Macquillan (1965) ve Newman (1967) tarafından verilmiştir.

$\Gamma(n)$, Γ'nın normal bir alt grubudur. Fakat genel olarak Γ'nın tüm denklik alt grupları, Γ da normal değildir.

$\Gamma(n)$'i elde etmenin diğer bir yolu da grubun tüm elemanlarını n modunda indirgeyen indirgeme homomorfizmasını kullanmaktır. Böylece $\Gamma(n)$ bu homomorfizmanın çekirdeğini oluşturur.

Parson (1976) tarafından p asal ve $m = 2,3$ olmak üzere $H(\sqrt{m})$'nin p seviyeli temel denklik alt grubu,

$$\Gamma_p(\sqrt{m}) = \{\, M \in H(\sqrt{m}) :\ M \equiv \pm I\ (mod\ p)\} \tag{1.3}$$

biçiminde tanımlanmıştır.

(1.3) eşitliğine denk olarak $H(\sqrt{m})$'nin p seviyeli temel denklik alt grubu yine Parson (1977) tarafından

$$\Gamma_p(\sqrt{m}) = \left\{T(z) = \frac{az+b\sqrt{m}}{c\sqrt{m}z+d} : a \equiv d \equiv \pm 1,\ b \equiv c \equiv 0\ (mod\ p),\ ad - mbc = 1\right\}$$

olarak tanımlanmıştır.

Genel olarak $q \in \mathbb{N}$, $q \geq 3$ ve p asal olmak üzere $H(\lambda_q)$'nun p seviyeli temel denklik alt grubu

$$\Gamma_p(\lambda_q) = \{\, T \in H(\lambda_q) : T \equiv \pm I\ (mod\ p)\,\}$$

$$= \left\{\begin{pmatrix} a & b\lambda \\ c\lambda & d \end{pmatrix} : a \equiv d \equiv \pm 1, b \equiv c \equiv 0\ (mod\ p), ad - \lambda^2 bc = 1\right\}$$

şeklinde tanımlanabilir.

$\Gamma_p(\lambda_q)$, her zaman $H(\lambda_q)$'nun normal bir alt grubudur.

Modüler grup durumunda p seviyeli temel denklik alt grubunun iki farklı şekilde verilen tanımlarının birbiriyle çakıştığını yukarıda belirttik. Acaba genelde diğer Hecke grupları için de iki farklı şekilde verilen bu alt grup tanımları çakışacak mıdır? Yoksa farklı iki alt grup mu ortaya çıkacaktır? Aşağıda bu soruya cevap arayacağız.

İndirgeme homomorfizmasını tanımlamanın genel olarak bir tek yolu olmadığından $q > 3$ için $H(\lambda_q)$'nun temel denklik alt gruplarını elde etmek çok daha karışıktır.

Tanım 1.4.1.3. $\wp$, $\mathbb{Z}[\lambda_q]$'nun bir ideali olmak üzere $\mathbb{Z}[\lambda_q]$ 'daki elemanları $mod\ \wp$'de indirgeyen

$$\Theta_\wp : \mathbb{Z}[\lambda_q] \rightarrow \mathbb{Z}[\lambda_q]/\wp$$

dönüşümü yardımıyla

$$H(\lambda_q) \rightarrow PSL(2, \mathbb{Z}[\lambda_q]/\wp\ )$$

dönüşümü elde edilir. Bu indirgeme homomorfizmasının çekirdeğine $\wp$ **seviyeli temel denklik alt grubu** denir.

s bir tam sayı olmak üzere $P_q^*(\lambda_q)$, $GF(p^s)$'de çözüme sahip olsun. Böyle bir s tam sayısı vardır ve $1 \leq s \leq d = \deg P_q^*(\lambda_q)$ özelliğini sağlar. O zaman u, $GF(p^s)$'de

$P_q^*(\lambda_q)$'nin bir çözümü olsun. $\wp$, $\mathbb{Z}[\lambda_q]$'da u tarafından üretilen bir ideal olmak üzere $\lambda_q \mapsto u$ dönüşümü tarafından indirgenen homomorfizm

$$\Theta_{p,u,q} : H(\lambda_q) \rightarrow PSL(2, p^s) \tag{1.4}$$

biçiminde tanımlanır. (1.4) dönüşümünün çekirdeği

$$K_{p,u}(\lambda_q) \coloneqq Ker(\Theta_{p,u,q})$$

olsun, $Ker(\Theta_{p,u,q})$, $H(\lambda_q)$'da normaldir.

Aşağıda Cangül (1993)'te Hecke gruplarının temel denklik alt grupları ile ilgili verilen bazı sonuçları, ileride bu konuda çalışacaklara yol gösterici olması ve bu tezin bütünlüğü açısından hatırlatacağız.

Verilen bir p için $K_{p,u}(\lambda_q)$, p ve u'ya bağlı olduğundan her bir u köküne karşılık farklı bir çekirdek gelebilir. Dolayısıyla Modüler grup durumundan farklı olarak diğer Hecke gruplarında temel denklik alt grubunun klasik tanımı ile indirgeme homomorfizmasının çekirdeği olarak elde edildiği tanım çakışmayabilir. Bazı durumlarda ise bu çekirdekler çakışabilir.

Aşağıdaki yardımcı teorem her bir u köküne karşı gelen çekirdeklerin bazı durumlarda çakıştığını belirtmektedir ki bu durumda klasik tanım indirgeme homomorfizmasının çekirdeği tanımı ile çakışmaktadır.

Yardımcı Teorem 1.4.1.4. (Cangul 1993) Eğer u ve v, $GF(p)$ üzerinde $P_q^*(\lambda_q)$'nun aynı indirgenemez f çarpanına karşılık gelirse $K_{p,u}(\lambda_q) = K_{p,v}(\lambda_q)$'dur.

u ve v, $P_q^*(\lambda_q)$'nun farklı çarpanlarına karşılık gelse bile $K_{p,u}(\lambda_q) = K_{p,v}(\lambda_q)$ olabilir.

Aşağıda bu durumu açıklayan bir örnek verilmiştir:

Örnek 1.4.1.5. $P_{17}^*(\sqrt{2})$ mod 17'deki iki kökü için sırasıyla $K_{17,6}(\sqrt{2}) - \Gamma_{17}(\sqrt{2})$ ve $K_{17,11}(\sqrt{2}) - \Gamma_{17}(\sqrt{2})$'deki tek elemanlar

$A = \begin{pmatrix} 224\sqrt{2} & 17 \\ 17 & 20\sqrt{2} \end{pmatrix}$ ve $B = \begin{pmatrix} 31\sqrt{2} & 17 \\ 51 & 14\sqrt{2} \end{pmatrix}$ olsun. A ve B tek elemanlarının nasıl bulunduğu daha sonra açıklanacaktır. O zaman

$$AB^{-1} = \begin{pmatrix} 224\sqrt{2} & 17 \\ 17 & 20\sqrt{2} \end{pmatrix} \begin{pmatrix} 14\sqrt{2} & -17 \\ -51 & 31\sqrt{2} \end{pmatrix} \equiv -I \ mod\ 17 \qquad (1.5)$$

denkliği geçerli olur. (1.5) bağıntısından da

$$A.\Gamma_{17}(\sqrt{2}) = B.\Gamma_{17}(\sqrt{2}) \qquad (1.6)$$

eşitliği sağlanır. Dolayısı ile (1.6) eşitliğinden de

$$K_{17,6}(\sqrt{2}) = K_{17,11}(\sqrt{2})$$

bağıntısı alınır.

Teorem 1.4.1.6. (Cangul 1993) $K_{p,u}(\lambda_q)$, $H(\lambda_q)$'nun p seviyeli normal bir denklik alt grubudur. Yani

$$\Gamma_p(\lambda_q) \trianglelefteq K_{p,u}(\lambda_q)$$

dir. Bundan dolayı da

$$\Gamma_p(\lambda_q) \leq \cap_{\forall u} K_{p,u}(\lambda_q)$$

özelliği sağlanır.

Aşağıda halka homomorfizmasından grup homomorfizmasının nasıl elde edildiği anlatılmaktadır:

$\mathcal{R}$ ve $\mathcal{S}$ iki birimli halka olmak üzere

$$\psi : \mathcal{R} \longrightarrow \mathcal{S}$$

dönüşümü bir halka homomorfizması olsun. O zaman ψ dönüşümü,

$$\overline{\psi} : SL(2,\mathcal{R}) \longrightarrow SL(2,\mathcal{S})$$

şeklindeki bir grup homomorfizmasına indirgenir.

Benzer olarak $PSL(2,\mathcal{R})$, $SL(2,\mathcal{R})$'nin merkeze yani $\pm I$'ya bölümü ile elde edilir. Böylece yine aynı ψ dönüşümü,

$$\underline{\psi} : PSL(2,\mathcal{R}) \longrightarrow PSL(2,\mathcal{S})$$

biçiminde diğer bir grup homomorfizmasına indirgenir.

Yukarıdaki gibi bir halka homomorfizmasından bir grup homomorfizması elde etme fikri, $H(\lambda_q)$ Hecke gruplarına da aşağıdaki biçimde uygulanabilir:

$\mathbb{Z}[\lambda_q]$, λ_q cebirsel sayısı ile tamsayılar halkasının bir genişlemesi olsun. p bir asal olmak üzere bu halkanın tüm elemanları p modunda indirgenirse $\mathbb{Z}[\lambda_q]$'nun tüm elemanlarını p modunda indirgeyen

$$\varphi_p : \mathbb{Z}[\lambda_q] \longrightarrow \mathbb{Z}_p[\lambda_q] \tag{1.7}$$

şeklinde bir halka homomorfizması elde edilir. $P_q^*(\lambda_q)$'nun var olan her bir $u \in GF(p)$ kökü için λ_q'yu $u \in GF(p)$ elemanına götüren

$$\chi_u : \mathbb{Z}_p[\lambda_q] \longrightarrow \mathbb{Z}_p = GF(p) \tag{1.8}$$

biçiminde bir halka homomorfizması vardır. $H_p(\lambda_q)$, R_p ve S_p tarafından üretilen p modundaki $H(\lambda_q)$'nun görüntüsünü göstermek üzere (1.7) ve (1.8)'deki iki halka homomorfizması

$$\underline{\varphi_p} : H(\lambda_q) < PSL(2,\mathbb{Z}[\lambda_q]) \longrightarrow H_p(\lambda_q) < PSL\,(2,\mathbb{Z}_p[\lambda_q]) \tag{1.9}$$

ve

$$\underline{\chi_u} : H_p(\lambda_q) < PSL\,(2,\mathbb{Z}_p[\lambda_q]) \longrightarrow PSL\,(2,p) \tag{1.10}$$

(1.9) ve (1.10) şeklinde iki grup homomorfizmasına indirgenir.

$P_q^*(\lambda_q)$'nun her bir $u \in GF(p)$ kökü için $K_{p,u}(\lambda_q)$,

$$\underline{\chi_u}\ o\ \underline{\varphi_p} : H(\lambda_q) \longrightarrow PSL\,(2,p)$$

bileşke homomorfizmasının çekirdeğini oluşturur.

Eğer u kökü $GF(p)$'de değilse o zaman $GF(p^s)$ cisim genişlemesindedir. O halde yukarıda yapılanlar $H(\lambda_q)$'dan $PSL\ (2, p^s)$'ye olan homomorfizmaya uygulanırsa bu dönüşümün çekirdeği $K_{p,u}(\lambda_q)$ olarak bulunur.

$P_q^*(\lambda_q)$ minimal polinomunun derecesi d ve her bir p_i, derecesi $d-1$'e eşit veya küçük olan λ_q'nun bir minimal polinomu olmak üzere $H(\lambda_q)$'nun bir T elemanı

$$T = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix}$$

biçimindedir. $\underline{\varphi_p}$ altında T, $\underline{T} = \begin{pmatrix} \underline{p_1} & \underline{p_2} \\ \underline{p_3} & \underline{p_4} \end{pmatrix}$ elemanına dönüşür. Burada $\underline{p_i}$, katsayıları $GF(p)$'de olan λ_q'nun polinomunu gösterir. Son olarak $\underline{p_i(u)}$, $u \in GF(p)$'de $\underline{p_i}$'nin değerlerini göstermek üzere $\underline{\chi_u}$ dönüşümü ile T, $PSL(2, p)$'deki

$$\underline{T_u} = \begin{pmatrix} \underline{p_1(u)} & \underline{p_2(u)} \\ \underline{p_3(u)} & \underline{p_4(u)} \end{pmatrix}$$

elemanına dönüşür.

Burada $P_q^*(\lambda_q)$'nun tüm köklerine karşılık gelen $K_{p,u}(\lambda_q)$'lar ile ilgilenilmeyecektir. Sadece s'nin olası en küçük değerleri için $GF(p^s)$'den seçilen u köklerine karşılık gelen $K_{p,u}(\lambda_q)$'lar ile ilgilenilecektir.

Örnek 1.4.1.7. $s = 1$ için $H(\lambda_q)$'dan $PSL\ (2, p)$'ye bir homomorfizma vardır. Bundan dolayı da $H(\lambda_q)$'nun $K_{p,u}(\lambda_q)$ ile bölümü daha sonra görüleceği gibi $PSL\ (2, p)$ olacaktır.

$\Gamma_p(\lambda_q)$'nun $K_{p,u}(\lambda_q)$'daki indeksi 1 değilse yani $\Gamma_p(\lambda_q)$ ve $K_{p,u}(\lambda_q)$ farklı ise $\Gamma_p(\lambda_q)$'yu hesaplamak için $K_{p,u}(\lambda_q)$ kullanılacaktır. Öncelikle tüm durumlarda $H(\lambda_q)$'nun $K_{p,u}(\lambda_q)$ ile bölümü belirlenecek daha sonra da bu bölüm kullanılarak istenilen $H(\lambda_q)$'nun $\Gamma_p(\lambda_q)$ ile bölümü elde edilecektir.

q'nun çeşitli değerleri için yani $q = 4$ ve 6 için $H(\lambda_q)$'nun $\Gamma_p(\lambda_q)$ ve $K_{p,u}(\lambda_q)$ ile bölümleri elde edilmiş ve bunlara ilişkin teoremler ispatları ile birlikte Cangül (1993) tarafından verilmiştir. Aşağıda bununla ilgili bilgiler hatırlanacaktır.

1.4.2. $H(\sqrt{2})$ ve $H(\sqrt{3})$'ün temel denklik alt grupları

Bu bölümde $m = 2$ ve 3 için Cangül (1993) tarafından verilen $H(\sqrt{m})$'nin temel denklik alt grupları ve bunların teorik grup yapısı ile ilgili bilgiler hatırlanacaktır.

Bu bilgiler ışığında öncelikle $H(\sqrt{m})$'nin $K_{p,u}(\sqrt{m})$ ile bölümü daha sonra da $H(\sqrt{m})$'nin $\Gamma_p(\sqrt{m})$ ile bölümü verilecektir.

Aşağıda $q = 4$ için Cangül (1993)'ün çalışmasında $H(\sqrt{2})$'nin denklik alt grupları ile ilgili verilen sonucu hatırlatıyoruz.

Teorem 1.4.2.1. $H(\sqrt{2})$ Hecke grubunun $K_{p,u}(\sqrt{2})$ ve $\Gamma_p(\sqrt{2})$ temel denklik alt grupları ile olan bölüm grupları

$$H(\sqrt{2})/K_{p,u}(\sqrt{2}) \cong \begin{cases} PSL(2,p) & p \equiv \pm 1 \mod 8 \\ PGL(2,p) & p \equiv \pm 3 \mod 8 \\ C_2 & p = 2 \end{cases}$$

ve

$$H(\sqrt{2})/\Gamma_p(\sqrt{2}) \cong \begin{cases} C_2 \times PSL(2,p) & p \equiv \pm 1 \mod 8 \\ PGL(2,p) & p \equiv \pm 3 \mod 8 \\ D_4 & p = 2 \end{cases}$$

şeklindedir.

Aşağıdaki Örnek 1.4.2.2. daha önce Örnek 1.4.1.5'te verilen tek elemanların elde edilişi ile ilgilidir.

Örnek 1.4.2.2. $p = 17$ olsun. O zaman $u = \sqrt{2} \equiv \pm 6 \ mod \ 17$'dir. $u \equiv 6 \ mod \ 17$ kökü seçilsin. $K_{17,6}(\sqrt{2}) - \Gamma_{17}(\sqrt{2})$ 'deki $A = \begin{pmatrix} x\sqrt{2} & y \\ z & t\sqrt{2} \end{pmatrix}$ tek matrisinin ne olduğu bulunmalıdır. Bu biçimdeki bir tek eleman

$$\Delta = 2xt - yz = 1 \qquad (1.11)$$

$$xu \equiv tu \equiv 1, \quad y \equiv z \equiv 0 \ \ mod \ 17$$

koşullarını sağlar.

$u \equiv 6 \ mod \ 17$ olduğundan

$$x \equiv t \equiv 20 \ \ mod \ 17 \qquad (1.12)$$

denkliği alınır. Buradan da a, b, c, d negatif olmayan tamsayılar olmak üzere (1.12), (1.11)'de yerine konulursa

$$2(20 + 17a)(20 + 17b) - 17c \cdot 17d = 1$$

eşitliği alınır. Böylece yapılan bir takım hesaplamalar sonucu

$$47 + 2 \cdot 20(a + b) + 2 \cdot 17ab = 17cd \qquad (1.13)$$

eşitliği elde edilir. (1.13) eşitliği

$$17 | \big(47 + 2 \cdot 20(a + b)\big) \qquad (1.14)$$

olduğunda bir çözüme sahiptir. (1.14)'te $k = 47$ ve $v = 20$ olarak bilindiğinden (1.14) sağlanacak şekilde negatif olmayan a ve b tamsayıları seçilebilir. (1.13) eşitliğinin sonsuz çoklukta çözümü olduğundan $b = 0$ ve $c = 1$ seçilerek

$$47 + 2 \cdot 20a = 17d \qquad (1.15)$$

eşitliği bulunur. (1.15) eşitliği de sadece $a = 12$ ve $d = 31$ için sağlanır. Dolayısı ile (1.13)'in özel bir çözümü

$$A = \begin{pmatrix} (20 + 17 \cdot 12)\sqrt{2} & 17 \\ 31 \cdot 17 & 20\sqrt{2} \end{pmatrix} = \begin{pmatrix} 224\sqrt{2} & 17 \\ 527 & 20\sqrt{2} \end{pmatrix}$$

şeklinde elde edilir. Yani $17 \equiv 1 \; mod \; 8$ olduğundan $K_{17,6}(\sqrt{2}) - \Gamma_{17}(\sqrt{2})$ 'deki A elemanı

$$A = \begin{pmatrix} 224\sqrt{2} & 17 \\ 17 & 20\sqrt{2} \end{pmatrix}$$

biçiminde bulunur.

$u \in GF(17)$'nin diğer 11 değeri seçilirse benzer şekilde yapılan hesaplamalar sonucu diğer tek eleman da yani $K_{17,11}(\sqrt{2}) - \Gamma_{17}(\sqrt{2})$'deki B elemanı da

$$B = \begin{pmatrix} 31\sqrt{2} & 17 \\ 51 & 14\sqrt{2} \end{pmatrix}$$

şeklinde elde edilir. Bu özel örnekte görüldüğü gibi $-11 \equiv 6 \; mod \; 17$ olduğundan bu iki u köküne karşılık gelen bu iki temel denklik alt grubundan birinin üreteci, diğerinin üretecinin tersidir. Bundan dolayı bu iki alt grup, $H(\sqrt{2})$'de birbirine izomorfiktir.

Aşağıda $q = 6$ için Cangül (1993)'ün çalışmasında verilen $H(\sqrt{3})$'ün temel denklik altgruplarının hesaplanışına ilişkin sonuç görülmektedir. $q = 6$ durumu, tamamen $q = 4$ durumuna benzerdir.

Teorem 1.4.2.3. $H(\sqrt{3})$ Hecke grubunun $K_{p,u}(\sqrt{3})$ ve $\Gamma_p(\sqrt{3})$ temel denklik altgrupları ile olan bölüm grupları

$$H(\sqrt{3})/K_{p,u}(\sqrt{3}) \cong \begin{cases} PSL(2,p) & p \equiv \pm 1 \; mod \; 12 \\ PGL(2,p) & p \not\equiv \pm 1 \; mod \; 12, \\ & p \neq 2 \\ C_2 & p = 3 \\ D_3 & p = 2 \end{cases}$$

ve

$$H(\sqrt{3})/\Gamma_p(\sqrt{3}) \cong \begin{cases} C_2 \times PSL(2,p) & p \equiv \pm 1 \; mod \; 12 \\ PGL(2,p) & p \not\equiv \pm 1 \; mod \; 12, \\ & p \neq 2 \\ (C_3 \times C_3) \wr C_2 & p = 3 \\ D_6 & p = 2 \end{cases}$$

şeklindedir.

Teorem 1.4.2.3'te $p = 3$ için $H(\sqrt{3})/\Gamma_p(\sqrt{3}) \cong (C_3 \times C_3) \wr C_2$ olup " $\wr$ " simgesi wreath çarpmını göstermektedir.

Aşağıda Teorem 1.4.2.3'ün uygulamasına ilişkin bir örnek verilmektedir. Burada yapılan hesaplamalar Örnek 1.4.2.2'dekine benzerdir.

Örnek 1.4.2.4. $p = 23$ olsun. O zaman $u = \sqrt{3} \equiv \pm 7 \ mod\ 23$'dir. $u \equiv 7 \ mod\ 23$ kökü seçilsin. $K_{23,7}(\sqrt{3}) - \Gamma_{23}(\sqrt{3})$ 'deki $A = \begin{pmatrix} x\sqrt{3} & y \\ z & t\sqrt{3} \end{pmatrix}$ tek matrisi şeklinde bulunmalıdır. Bu biçimdeki bir tek eleman

$$\Delta = 3xt - yz = 1 \tag{1.16}$$

$$xu \equiv tu \equiv 1, \quad y \equiv z \equiv 0 \ mod\ 23$$

koşullarını sağlar.

$u \equiv 7 \ mod\ 23$ olduğundan

$$x \equiv t \equiv 10 \ mod\ 23 \tag{1.17}$$

denkliği alınır. Buradan da a, b, c, d negatif olmayan tamsayılar olmak üzere (1.17), (1.16)'da kullanıldığında

$$3(10 + 23a)(10 + 23b) - 23c \cdot 23d = 1$$

eşitliği alınır. Böylece yapılan bir takım hesaplamalar sonucu

$$13 + 3 \cdot 10(a + b) + 3 \cdot 23ab = 23cd \tag{1.18}$$

eşitliği elde edilir. (1.18) eşitliği

$$23 | (13 + 3 \cdot 10(a + b)) \tag{1.19}$$

olduğunda bir çözüme sahiptir. (1.19)'da $k = 13$ ve $v = 10$ olarak bilindiğinden (1.19) sağlanacak şekilde negatif olmayan a ve b tamsayıları seçilebilir. (1.18) eşitliğinin sonsuz çoklukta çözümü olduğundan $b = 0$ ve $c = 1$ seçilerek

$$13 + 3.10a = 23d \tag{1.20}$$

eşitliği bulunur. (1.20) eşitliği de sadece $a = 8$ ve $d = 11$ için sağlanır. Dolayısı ile (1.18)'in özel bir çözümü

$$A = \begin{pmatrix} (10 + 23 \cdot 8)\sqrt{3} & 23 \\ 11 \cdot 23 & 10\sqrt{3} \end{pmatrix} = \begin{pmatrix} 194\sqrt{3} & 23 \\ 253 & 10\sqrt{3} \end{pmatrix}$$

şeklinde elde edilir. Yani $23 \equiv -1 \ mod \ 12$ olduğundan $K_{23,7}(\sqrt{3}) - \Gamma_{23}(\sqrt{3})$'teki A tek elemanı

$$A = \begin{pmatrix} 224\sqrt{3} & 23 \\ 253 & 10\sqrt{3} \end{pmatrix}$$

biçiminde bulunur.

Aşağıdaki sonuç Cangül (1993) tarafından verilmiş olup $m = 2$ ve 3 için $H(\sqrt{m})$'nin $K_{p,u}(\sqrt{m})$ ve $\Gamma_p(\sqrt{m})$ denklik alt gruplarının indeksleri hakkında bilgi vermektedir.

Sonuç 1.4.8.5. $H(\sqrt{m})$'nin $K_{p,u}(\sqrt{m})$ ve $\Gamma_p(\sqrt{m})$ denklik alt gruplarının indeksler formülü

$$|H(\sqrt{m})/K_{p,u}(\sqrt{m})| = \begin{cases} p(p-1)(p+1)/2 & m\,, mod\ p'de\ karesel \\ & ve\ p \neq m \\ p(p-1)(p+1) & m\,,\ mod\ p'de\ karesel\ değil \\ & ve\ p \neq 6/m \\ 2 & p = m \\ 24 & m = 2, p = 3 \\ 6 & m = 3, p = 2 \end{cases}$$

ve

$$|H(\sqrt{m})/\Gamma_p(\sqrt{m})| = \begin{cases} p(p-1)(p+1) & p \neq m, 6/m \\ 2m^2 & p = m \\ 24 & m = 2, p = 3 \\ 12 & m = 3, p = 2 \end{cases}$$

biçimindedir.

Cangül (1993)'teki çalışmasında $m = 2$ ve 3 için $H(\sqrt{m})$'nin $K_{p,u}(\sqrt{m})$ ve $\Gamma_p(\sqrt{m})$ alt gruplarının teorik grup yapısı hakkında bilgiler vermiştir. Burada bu alt gruplara ilişkin birkaç örnek verilecektir. Öncelikle $H(\sqrt{2})$ durumundaki grup yapısı ile ilgili örnek verilecektir.

Örnek 1.4.2.6. $p = 17$ olsun. O zaman $17 \equiv 1 \, mod \, 8$'dir. Bu durumda Teorem 1.4.2.1'e göre $H(\sqrt{2})$'nin $K_{17,u}(\sqrt{2})$ ve $\Gamma_{17}(\sqrt{2})$ ile bölüm grupları sırasıyla $PSL(2,17)$ ve $C_2 \times PSL(2,17)$ dir. Buna göre $K_{p,u}(\sqrt{2})$ ve $\Gamma_p(\sqrt{2})$'nin gösterimleri

$$g = 1 + \frac{\mu}{8p}(p-4)$$

olmak üzere $\left(g\,;\,\infty^{(\mu/p)}\right)$ şeklindedir.

Öncelikle Teorem 1.4.2.5 gereğince $\sqrt{2} \equiv 6 \, mod \, 17$ karesel olduğundan $K_{17,6}(\sqrt{2}) = K_{17,11}(\sqrt{2})$'nin μ indeksi $17{\cdot}16{\cdot}9 = 2448$'dur. Buradan $K_{17,6}(\sqrt{2}) = K_{17,11}(\sqrt{2})$'nin cinsi

$$g = 1 + \frac{17{\cdot}16{\cdot}9}{8{\cdot}17}(17-4) = 235$$

biçiminde bulunur. Dolayısı ile de $K_{17,6}(\sqrt{2}) = K_{17,11}(\sqrt{2})$'nin gösterimi

$$\left(235\,;\,\infty^{(17\cdot16\cdot9/17)}\right) = \left(235\,;\,\infty^{(144)}\right)$$

şeklinde alınır. Benzer olarak Teorem 1.4.2.5 gereğince $\Gamma_{17}(\sqrt{2})$'nin μ indeksi $17{\cdot}16{\cdot}18 = 4896$'dir. $\Gamma_{17}(\sqrt{2})$'nin cinsi

$$g = 1 + \frac{17{\cdot}16{\cdot}18}{8{\cdot}17}(17-4) = 469$$

şeklinde bulunur. Böylece $\Gamma_{17}(\sqrt{2})$'nin gösterimi

$$\left(469\,;\,\infty^{(17\cdot16\cdot18/17)}\right) = \left(469\,;\,\infty^{(288)}\right)$$

biçimindedir.

Örnek 1.4.2.6'dan $K_{p,u}(\sqrt{2})$ ve $\Gamma_p(\sqrt{2})$'nin cinsleri ve parabolik sınıf sayıları arasında aşağıdaki bağıntılar geçerlidir. Buna göre $K_{p,u}(\sqrt{2})$'nin cinsi g_k, parabolik sınıf sayısı t_k ve $\Gamma_p(\sqrt{2})$'nin cinsi g_γ, parabolik sınıf sayısı t_γ olmak üzere

$$g_\gamma = 2 \cdot g_k - 1$$

ve

$$t_k = 2 \cdot t_\gamma$$

bağıntıları geçerlidir.

Şimdi de $H(\sqrt{3})$ durumundaki grup yapısı ile ilgili örnek verilecektir.

Örnek 1.4.2.7. $p = 23$ olsun. O zaman $23 \equiv -1 \; mod \; 12$'dir. Bu durumda Teorem 1.4.2.3'e göre $H(\sqrt{3})$'ün $K_{p,u}(\sqrt{3})$ ve $\Gamma_p(\sqrt{3})$ ile bölüm grupları sırasıyla $PSL(2,p)$ ve $C_2 \times PSL(2,p)$ biçimindedir. Yani $H(\sqrt{3})/K_{p,u}(\sqrt{3}) \cong PSL(2,p)$ ve$H(\sqrt{3})/\Gamma_p(\sqrt{3}) \cong C_2 \times PSL(2,p)$'dir. Buna göre $K_{p,u}(\sqrt{3})$ ve $\Gamma_p(\sqrt{3})$'ün gösterimleri

$$g = 1 + \frac{\mu}{6p}(p-3)$$

olmak üzere $\left(g \; ; \; \infty^{(\mu/p)}\right)$ şeklindedir.

Öncelikle Teorem 1.4.2.5 gereğince $\sqrt{3} \equiv 7 \; mod \; 23$ karesel olduğundan $K_{23,6}(\sqrt{3}) = K_{23,11}(\sqrt{3})$'nin μ indeksi $23 \cdot 22 \cdot 12 = 6072$'dir. Buradan $K_{23,7}(\sqrt{3}) = K_{23,16}(\sqrt{3})$'nin cinsi

$$g = 1 + \frac{23 \cdot 22 \cdot 12}{6 \cdot 23}(23-3) = 881$$

dir. Dolayısı ile de $K_{23,7}(\sqrt{3}) = K_{23,16}(\sqrt{3})$'nin gösterimi

$$\left(881 \; ; \; \infty^{(23 \cdot 22 \cdot 12/23)}\right) = \left(881 \; ; \; \infty^{(264)}\right)$$

şeklinde alınır. Benzer olarak Teorem 1.4.2.5 gereğince $\Gamma_{23}(\sqrt{3})$ 'ün μ indeksi $23 \cdot 22 \cdot 24 = 12144$'tür. $\Gamma_{23}(\sqrt{3})$'ün cinsi

$$g = 1 + \frac{23 \cdot 22 \cdot 24}{6 \cdot 23}(23 - 3) = 1761$$

şeklinde bulunur. Böylece $\Gamma_{23}(\sqrt{3})$'nin gösterimi

$$\left(1761\,;\,\infty^{(23 \cdot 22 \cdot 24/23)}\right) = \left(1761\,;\,\infty^{(528)}\right)$$

biçimindedir.

Aşağıda Cangül (1993) tarafından verilen $q = 5$ değeri için $H(\lambda_5)$ Hecke grubunun temel denklik altgrupları ile ilgili bilgiler hatırlanacaktır.

1.4.3. $H(\lambda_5)$'nin temel denklik alt grupları

$q = 5$ için $x^2 - x - 1 = 0$ minimal polinomunun kökü, altın oran olarak bilinen $\lambda = \lambda_5 = \frac{1+\sqrt{5}}{2}$ sayısıdır. $\lambda^2 = \lambda + 1$ olduğundan $\mathbb{Q}(\lambda)$'nın her elemanı λ'ya göre doğrusaldır. Yani $a, b \in \mathbb{Q}$ olmak üzere $\mathbb{Q}(\lambda)$'nın her elemanı $a\lambda + b$ biçimindedir. Bundan dolayı $a, b \in \mathbb{Z}$ olmak üzere $H(\lambda_5)$ Hecke grubunun dönüşümlerinin tüm katsayıları $a\lambda + b$ biçiminde olacaktır.

$H(\lambda_5)$ Hecke grubunun

$$R^2 = S^5 = I$$

bağıntısını sağlayan

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\; S = \begin{pmatrix} 0 & -1 \\ 1 & \lambda_5 \end{pmatrix}$$

şeklindeki matrislere karşılık gelen elemanlar tarafından üretildiği bilinmektedir.

$H(\lambda_5)$ Hecke grubunun denklik alt grupları şu biçimde elde edilir:

Bir p asalı için $H(\lambda_5)$ Hecke grubunun tüm elemanları asal modda indirgenir. Bu indirgeme ile $H(\lambda_5)$'ten $H(\lambda_5)\,/K_{p,u}(\lambda_5)$ bölüm grubuna bir homomorfizma elde edilir. Bu homomorfizma ile R, S ve T elemanları r_p, s_p ve t_p elemanlarına dönüşür. Böylece $H(\lambda_5)\,/K_{p,u}(\lambda_5)$,

$$\langle r_p,\ s_p\ :\ r_p^2 = s_p^5 = t_p^p = I,\ t_p = r_p s_p \rangle$$

biçimindeki grubun homomorfik bir görüntüsü olur.

$H(\lambda_5)$ Hecke grubunun denklik alt gruplarının elde edilmesi ile ilgili olası durumlar Cangül (1993) tarafından incelenmiş ve aşağıdaki sonuç bulunmuştur.

Teorem 1.4.3.1. $H(\lambda_5)$ Hecke grubunun $K_{p,u}(\lambda_5)$ temel denklik alt grubu ile olan bölüm grupları

$$H(\lambda_5)\ /K_{p,u}(\lambda_5) = \begin{cases} PSL(2,p) & p \equiv \pm 1\ mod\ 10, \\ PSL(2,p^2) & p \equiv \pm 3\ mod\ 10, \\ & p \neq 3, \\ D_5 & p = 2, \\ A_5 & p = 3, 5 \end{cases}$$

şeklindedir.

Aşağıdaki örnek Teorem 1.4.3.1'in uygulaması niteliğindedir.

Örnek 1.4.3.2. $p = 41$ olsun. $41 \equiv 1\ mod\ 10$ ve $5\ mod\ 41$'de karesel olduğundan $\sqrt{5} \in GF(41)$ 'dir. $P_5^*(\lambda_5) = {\lambda_5}^2 - \lambda_5 - 1$ ikinci dereceden minimal polinom olduğundan $P_5^*(\lambda_5)$'e karşılık gelen iki kök vardır. $7^2 - 7 - 1 = 41 \equiv 0\ mod\ 41$ olduğundan $u = 7$ ve $35^2 - 35 - 1 = 1189 = 29 \cdot 41 \equiv 0\ mod\ 41$ olduğundan $v = 35$ olmak üzere λ_5'in 41 modunda iki değeri vardır. Buradan da $\lambda_5 \longrightarrow 7$ ve $\lambda_5 \longrightarrow 35$ dönüşümleri tarafından indirgenen

$$\theta_i : H(\lambda_5) \longrightarrow PSL(2,p)\ ,\ i = 1,2$$

biçiminde iki homomorfizma elde edilir. Dolayısı ile $H(\lambda_5)$ Hecke grubunun, 7 ve 35 köklerine karşılık gelen $K_{41,7}(\lambda_5)$ ve $K_{41,35}(\lambda_5)$ şeklinde iki çekirdeği elde edilir. Bu da $H(\lambda_5)$ Hecke grubunun $K_{41,7}(\lambda_5)$ ve $K_{41,35}(\lambda_5)$ şeklinde iki normal denklik alt grubuna sahip olması anlamına gelmektedir.

Aşağıda $H(\lambda_5)$'teki $K_{p,u}(\lambda_5)$ çekirdeğinin teorik grup yapısını hatırlatıcı bazı bilgiler verilmektedir.

$H(\lambda_5)\ /K_{p,u}(\lambda_5)$ bölüm grubunda

$$r_p^2 = s_p^5 = I$$

bağıntısı geçerli olduğundan tüm alt gruplar serbesttir. Buna ek olarak $t_p^p = I$ olduğundan $K_{p,u}(\lambda_5)$, p seviyedendir. Permutasyon metodu ve Riemann-Hurwitz formülünden $K_{p,u}(\lambda_5)$,

$$\left(1 + \frac{\mu}{20p}(3p - 10)\ ;\ \infty^{(\mu/p)}\right) \tag{1.21}$$

biçiminde bir gösterime sahiptir.

Aşağıdaki örnek $K_{41,7}(\lambda_5)$ çekirdeğinin gösterimi ile ilgilidir.

Örnek 1.4.3.3. $H(\lambda_5)\ /K_{41,u}(\lambda_5)$ bölüm grubunun indeksi $41{\cdot}40{\cdot}21 = 34440$ 'dır. Dolayısı ile (1.21)'den $K_{41,u}(\lambda_5)$,

$$\left(4747\ ;\ \infty^{(840)}\right)$$

şeklinde bir gösterime sahiptir. Yani $K_{41,u}(\lambda_5) \cong \left(4747\ ;\ \infty^{(840)}\right)$'dır.

Buraya kadar yapılan hatırlatmaları kısaca özetlemek gerekir. $q = 4$ ve 6 için $K_{p,u}(\sqrt{m})$ çekirdeğinin nasıl elde edildiği, bu çekirdek yardımıyla $\Gamma_p(\sqrt{m})$ temel denklik altgruplarının nasıl bulunduğu hatırlatıldı. Daha sonra da p asalının çeşitli değerleri için bu denklik alt gruplarının farklı olduğu ve sonra da $H(\lambda_5)$'in temel denklik alt gruplarının nasıl elde edildiği hatırlatıldı. $q = 4$ ve 5 durumlarının aksine $p \equiv \pm 1\ mod\ 10$ durumu için $H(\lambda_5)$'in $K_{p,u}(\lambda_5)$ biçiminde iki altgruba sahip olduğu görüldü.

1.4.4. Diğer Hecke gruplarının temel denklik alt grupları

$q = 3, 4, 5$ ve 6 durumları için Cangül (1993) tarafından verilen sonuçlar, bu kısma kadar açıklayıcı örneklerle desteklendi. Şimdi de $q \geq 7$ asal olması durumunda yine Cangül (1993) tarafından verilen sonuçlar hatırlanacaktır. Burada $q = 7$ durumu,

$H(\lambda_q)\,/K_{p,u}(\lambda_q)$ bölüm grubunun Hurwitz grubuna denk olması açısından dikkate değerdir. Aslında $p = 2$ dışındaki bölümlerin tümü, Hurwitz grubuna denktir.

Aşağıda Cangül (1993) tarafından verilen sonuç, p'nin tüm olası durumları için $H(\lambda_7)$'nin temel denklik alt gruplarını vermektedir.

Teorem 1.4.4.1. $H(\lambda_7)$ Hecke grubunun $K_{p,u}(\lambda_7)$ temel denklik alt grubu ile olan bölüm grupları

$$H(\lambda_7)\,/K_{p,u}(\lambda_7) = \begin{cases} D_7 & p = 2 \\ PSL(2,7) & p = 7 \\ PSL(2,p) & p \equiv \pm 1 \ mod\ 7 \\ PSL(2,p^n) & p \not\equiv \pm 1\ \ mod\ 7,\ p \neq 2 \end{cases}$$

biçimindedir.

Örnek 1.4.4.2. $p = 29$ olsun. O zaman $29 \equiv 1\ mod\ 7$'tür. 7 asal olduğundan bu denklik, $29 \equiv 1\ mod\ 14$ ifadesiyle aynı anlama gelir. Buradan da $P_7^*(\lambda_7) = {\lambda_7}^3 - {\lambda_7}^2 - 2\lambda_7 + 1$ üçüncü dereceden minimal polinom olduğundan $P_7^*(\lambda_7)$'e karşılık gelen üç kök vardır. $11^3 - 11^2 - 2{\cdot}11 + 1 = 1189 = 29{\cdot}41 \equiv 0\ mod\ 29$ olduğundan $u = 11 \in GF(29)$, $22^3 - 22^2 - 2{\cdot}22 + 1 = 10121 = 29{\cdot}349 \equiv 0\ mod\ 29$ olduğundan $v = 22 \in GF(29)$ ve $26^3 - 26^2 - 2{\cdot}26 + 1 = 16849 = 29{\cdot}581 \equiv 0\ mod\ 29$ olduğundan $t = 26 \in GF(29)$ olmak üzere λ_7'nin 29 modunda üç değeri vardır. Buradan da $\lambda_7 \longrightarrow 11$, $\lambda_7 \longrightarrow 22$ ve $\lambda_7 \longrightarrow 26$ dönüşümleri tarafından indirgenen

$$\theta_i : H(\lambda_7) \longrightarrow PSL(2,p)\ ,\ i = 1,2,3$$

biçiminde üç homomorfizma elde edilir. Dolayısı ile $H(\lambda_7)$ Hecke grubunun 11, 22 ve 26 köklerine karşılık gelen $K_{29,11}(\lambda_7)$, $K_{29,22}(\lambda_7)$ ve $K_{29,26}(\lambda_7)$ şeklinde üç çekirdeği elde edilir. Bu da $H(\lambda_7)$ Hecke grubunun $K_{29,11}(\lambda_7)$, $K_{29,22}(\lambda_7)$ ve $K_{29,26}(\lambda_7)$şeklinde üç tane normal denklik alt grubuna sahip olması anlamına gelmektedir.

Örnek 1.4.4.2'de $q = 7$ ve $p \equiv \pm 1\ mod\ 7$ durumu için $GF(p)$'de $P_7^*(x)$'in her bir köküne karşılık $H(\lambda_7)$'den $PSL(2,p)$'ye üç homomorfizma elde edildi. Bu homomorfizmalardan da $H(\lambda_7)$'nin eşlenik olmayan üç normal alt grubu bulundu. Benzer işlemler $q > 7$ olduğunda da yapılabilir. Her seferinde $P_q^*(x)$ asal p modunda indirgenir. Sonra da $P_q^*(x)$, ya $GF(p)$'de ya da $GF(p)$'nin sonlu genişlemesinde parçalanır. Yani $P_q^*(x)$'ın asal p modundaki kökleri ya $GF(p)$'de ya da $GF(p)$'nin sonlu genişlemesindedir. Eğer özel bir u kökü $GF(p)$'de ise o zaman $H(\lambda_q)$'dan $PSL(2,p)$'ye bir homomorfizma vardır ve bu homomorfizmanın çekirdeği de $K_{p,u}(\lambda_q)$'dur. Benzer şekilde n, $P_q^*(x)$ minimal polinomunun d derecesine eşit veya d derecesinden küçük olmak üzere eğer $u \in GF(p^n)$ ise o zaman $K_{p,u}(\lambda_q)$ çekirdekli $H(\lambda_q)$ 'dan $PSL(2,p^n)$'ye bir homomofizma vardır. Böylece her bir u köküne karşılık başka bir $K_{p,u}(\lambda_q)$ normal alt grubu elde edilir.

Aşağıdaki sonuç Cangül (1993) tarafından elde edilmiş olup $q > 7$ tek asal olması durumundaki $H(\lambda_q)$'nun denklik alt grubunu vermektedir.

Teorem 1.4.4.3. Eğer $p \equiv \pm 1 \ mod \ q$ ise her bir $u \in GF(p)$ köküne karşılık

$$\theta : \ H(\lambda_q) \ \longrightarrow PSL(2,p)$$

şeklinde bir homomomorfizma vardır ve bu homomorfizmanın çekirdeği $K_{p,u}(\lambda_q)$'dur.

2. ψ_{2q} VE λ_q'NUN MİNİMAL POLİNOMLARI

2.1. Giriş

Bilinen ilk dört Hecke grubu olan Γ, $H(\sqrt{2})$, $H(\lambda_5)$ ve $H(\sqrt{3})$ için $\mathbb{Q}$ üzerinde λ_q'nun minimal polinomları sırasıyla $\lambda_3 - 1$, $\lambda_4^2 - 2$, $\lambda_5^2 - \lambda_5 - 1$ ve $\lambda_6^2 - 3$'tür. Görüldüğü gibi q < 7 iken $\mathbb{Q}$ üzerinde λ_q'nun minimal polinomlarını elde etmek ve bununla birlikte bu polinomların asal moddaki köklerini bulmak oldukça kolaydır. Buna karşın $q \geq 7$ olduğunda $q \in \mathbb{N}$ olmak üzere $\lambda_q = 2cos\,\pi/q$ cebirsel sayısı, derecesi 3 ve 3'ten büyük olan bir minimal polinomun köküdür. Bundan dolayı da $q \geq 7$ olduğunda λ_q'nun minimal polinomlarını ilk dört durumda olduğu gibi elde etmek kolay değildir. Cangül (1993) çalışmasında $q \geq 7$ olduğunda q'nun tek ve çift olduğu durumlar için λ_q'nun minimal polinomlarınını elde etmeyi başarmıştır. Bu tez çalışmasının bu bölümünde $q \in \mathbb{N}$, $q \geq 3$ olmak üzere $\lambda_q = 2cos\,\pi/q$ cebirsel sayısının minimal polinomunun asal moddaki kökleri ile ilgili sonuçlar elde edilecektir. Bu sonuçlar, ayrık gruplar teorisinde önemli bir problem olan Hecke gruplarının denklik alt gruplarının hesaplanmasında yarar sağlayacaktır.

Cangül (1993) çalışmasında λ_q'nun minimal polinomları için verdiği formüllerde $\mathbb{Q}$ üzerinde $x = \cos\pi/q$ 'nun ψ_{2q} minimal polinomları dikkati çekmektedir. Bu polinomların hesabı Watkins ve Zeitlin (1993) tarafından Chebycheff polinomları yardımı ile yapılmıştır. Cangül (1993) çalışmasında da $2q = n$ olmak üzere $1 \leq n \leq 13$ için $\psi_n(x)$ polinomlarını vermiştir. $n > 13$ durumunda $\psi_n(x)$ polinomlarının hesabını el ile yapmak oldukça zor ve zaman alıcıdır. Bundan dolayı bu tez çalışmasında $n > 13$ durumunda $\psi_n(x)$ polinomlarının hesabının nasıl yapıldığı MAPLE adlı matematiksel yazılımı kullanılarak anlatılacaktır. Böylece $q > 7$ durumundaki $\mathbb{Q}$ üzerinde λ_q'nun minimal polinomlarının hesaplanması kolaylaşacaktır.

Bu bölümde yapılan hesaplamalarda MAPLE'ın seçilmesinin sebebi, Maple'ın dünya çapında, eğitimde, araştırmalarda ve sanayide kullanılan güçlü bir matematiksel problem çözme ve görüntüleme sisteminin olmasıdır. En güçlü özelliği ise sembolik problem çözme algoritmalarıdır. Sadece yüzeysel-nokta sayıları ile çalışabilen geleneksel matematik yazılımlarının aksine, Maple formal matematiksel ifadeler kullanarak problem çözebilir ve cevapları matematiksel objeler olarak verebilir.

Cangül (1993) çalışmasında $q \leq 50$ için λ_q'nun minimal polinomlarının bir listesini vermiştir. Fakat $q > 50$ durumunda λ_q 'nun minimal polinomlarını program kullanmadan yapmak oldukça güç ve zaman alıcıdır. Bu sebeple bu tez çalışmasında daha önce Cangül (1993) tarafından yapılan listeyi genişletmek amacıyla $q > 50$ durumunda bu minimal polinomlarını hesabının nasıl yapıldığı MAPLE kullanılarak anlatılacaktır. Böylece genişleyen bu liste daha pek çok çalışmanın önünü açacaktır.

Çalışmanın bu bölümünde öncelikle Chebycheff polinomları daha sonra Dickson polinomları ve en sonunda da $\psi_n(x)$ polinomları ilgili hatırlatmalar yapılmıştır. Buna ek olarak Chebycheff ve Dickson polinomlarının genişleyen listeleri MAPLE kullanılarak hesabının nasıl yapıldığı anlatılmıştır ve bu polinomların MAPLE'da yazılan algoritmaları verilmiştir. Böylece istenilen listeler, saniyeler gibi kısa bir zaman içinde MAPLE tarafından verilir.

2.2. Chebycheff Polinomları

Tanım 2.2.1. $n \in \mathbb{N}$ için $x, \theta \in \mathbb{R}$, $|x| \leq 1$ olmak üzere

$$T_n(x) \coloneqq cos(ncos^{-1}x)$$

veya $\theta \in \mathbb{R}$ olmak üzere

$$T_n(cos\theta) \coloneqq cos(n\theta)$$

biçiminde tanımlı $T_n(x)$ polinomuna ***n*. Chebycheff polinomu** adı verilir. $deg\big(T_n(x)\big) = n$'dir.

Bazı $T_n(x)$ polinomları aşağıda verilmiştir.

$$T_0(x) = 1,$$

$$T_1(x) = x,$$

$$T_2(x) = 2x^2 - 1,$$

$$T_3(x) = 4x^3 - 3x,$$

$$T_4(x) = 8x^4 - 8x^2 + 1.$$

Cangül (1993) tarafından $0 \leq n \leq 17$ için $T_n(x)$ polinomlarının bir listesi verilmiştir. Bu tez çalışmasında ise hesaplamayı kısa bir sürede yapabilen MAPLE kullanılarak $n > 17$ için $T_n(x)$ polinomlarının genişleyen bir listesi elde edilmiştir. Bu çalışmada bu liste çok uzun olduğu için sınırlandırma gereği duyulmuştur ve sadece $0 \leq n \leq 100$ için $T_n(x)$ polinomlarının listesi verilmiştir.

Aşağıda bu polinomların MAPLE kullanılarak nasıl elde edildiği anlatılmıştır.

Bazı polinomlar, MAPLE tarafından bilinmekte olup bu polinomlar " $[G, H, L, P, T, U]$ " isimli paket içindedir. Chebycheff polinomları da bu paket içinde olup " T " ile gösterilir. Bu polinomların uygun bir döngü altında hesaplanabilmesi için öncelikle bu paketin çağrılması gerekmektedir. Paketin çağrılmasından sonra $n \in \mathbb{N}$ için yazılan döngü ile program tarafından Chebycheff polinomlarının hesabı yapılır. Burada bu döngü sadece $0 \leq n \leq 100$ için yapılmıştır. Aşağıda "for" döngüsü içindeki "`print(n,sort(T(n,x)))`" komutunda virgülden önceki sayı n'i; sonraki polinom olan **`T(n,x)`** ise n-inci Chebycheff polinomunu göstermektedir.

```
> with(orthopoly);
```

$$[G, H, L, P, T, U]$$

```
> f:=proc(x)local n;with(orthopoly);for n from 0 to 100 do
print(n,sort(T(n,x)));end do;end proc;
```

```
f := proc(x)
local n;
    with(orthopoly); for n from 0 to 100 do print(n, sort(T(n, x))) end do
end proc
```

```
> f(x);
```

$$0, 1$$

$$1, x$$

$$2, 2x^2 - 1$$

$$3, 4x^3 - 3x$$

$$4, 8x^4 - 8x^2 + 1$$

$$5, 16x^5 - 20x^3 + 5x$$

$$6,\ 32\,x^6 - 48\,x^4 + 18\,x^2 - 1$$

$$7,\ 64\,x^7 - 112\,x^5 + 56\,x^3 - 7\,x$$

$$8,\ 128\,x^8 - 256\,x^6 + 160\,x^4 - 32\,x^2 + 1$$

$$9,\ 256\,x^9 - 576\,x^7 + 432\,x^5 - 120\,x^3 + 9\,x$$

$$10,\ 512\,x^{10} - 1280\,x^8 + 1120\,x^6 - 400\,x^4 + 50\,x^2 - 1$$

$$11,\ 1024\,x^{11} - 2816\,x^9 + 2816\,x^7 - 1232\,x^5 + 220\,x^3 - 11\,x$$

$$12,\ 2048\,x^{12} - 6144\,x^{10} + 6912\,x^8 - 3584\,x^6 + 840\,x^4 - 72\,x^2 + 1$$

$$13,\ 4096\,x^{13} - 13312\,x^{11} + 16640\,x^9 - 9984\,x^7 + 2912\,x^5 - 364\,x^3 + 13\,x$$

$$14,\ 8192\,x^{14} - 28672\,x^{12} + 39424\,x^{10} - 26880\,x^8 + 9408\,x^6 - 1568\,x^4 + 98\,x^2 - 1$$

$$15,\ 16384\,x^{15} - 61440\,x^{13} + 92160\,x^{11} - 70400\,x^9 + 28800\,x^7 - 6048\,x^5 + 560\,x^3 - 15\,x$$

$$\vdots$$

Aşağıdaki yardımcı teorem Chebycheff polinomları arasında iyi bilinen bir indirgeme bağınıtısıdır.

Yardımcı Teorem 2.2.2. $n \in \mathbb{N}$ olmak üzere

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$$

bağıntısı geçerlidir.

2.3. Dickson Polinomları

$n \in \mathbb{N}$, $|x| \leq 2$, $x, \theta \in \mathbb{R}$, $x = D_1(x) = 2cos\theta$ olmak üzere

$$\begin{aligned} D_n(x) &= 2T_n(x/2) \\ &= 2cos\left(ncos^{-1}(x/2)\right) \qquad (2.1) \\ &= 2cosn\theta \end{aligned}$$

biçiminde geçerli olan eşitlik, Chebycheff polinomlarının normalizasyonu olarak bilinir. Bu polinomların normalizasyonu D_n ile gösterilir.

(2.1)'de $\theta = \pi/q$, $q \in \mathbb{N}$, $q \geq 3$ olsun. O zaman $x = \lambda_q$ olmak üzere $D_n(x)$, λ_q'nun bir polinomu olur. Gerçekten de $\zeta = e^{i\pi/q}$ olmak üzere

$$D_n(\lambda_q) = 2cos\frac{n\pi}{q} = \zeta^n + \zeta^{-n}$$

eşitliği geçerlidir.

Tanım 2.3.1. $[\alpha]$, α'ya eşit veya α'dan küçük en büyük tam sayıyı göstermek üzere

$$D_n(x) := \sum_{i=0}^{[n/2]}(-1)^i \frac{n}{n-i}\binom{n-i}{n} x^{n-2i} \tag{2.2}$$

$$= x^n - nx^{n-2} + \frac{n(n-3)}{2!}x^{n-4} - \frac{n(n-4)(n-5)}{3!}x^{n-6} + \cdots$$

biçiminde Weber (1898) tarafından açıkça tanımlanan polinomlara **Dickson polinomları** adı verilir. Ayrıca

$$deg(D_n(x)) = n$$

dir.

Aşağıdaki yardımcı teorem Dickson polinomları için bir indirgeme bağıntısıdır.

Yardımcı Teorem 2.3.2. $n \in \mathbb{N}$ ve $D_0(x) = 1$ olsun. O zaman

$$D_2(x) = xD_1(x) - 2D_0(x)$$

$$D_{n+1}(x) = xD_n(x) - D_{n-1}(x), n > 1$$

eşitlikleri geçerlidir.

Bazı Dickson polinomları aşağıda verilmiştir.

$$D_1(x) = x,$$

$$D_2(x) = x^2 - 2,$$

$$D_3(x) = x^3 - 3x,$$

$$D_4(x) = x^4 - 4x^2 + 2,$$

$$D_5(x) = x^5 - 5x^3 + 5x\ .$$

Cangül (1993) çalışmasında $0 \leq n \leq 32$ için Dickson polinomlarının bir listesini vermiştir. Fakat n'nin artan doğal sayı değerleri için bu polinomların hesabını yapmak giderek zorlaşmakta ve zaman kaybına sebep olmaktadır. Bu sebeple bu tez çalışmasının bu bölümünde $n \in \mathbb{N}$ için $D_n(x)$ polinomlarının hesabı MAPLE kullanılarak kolaylıkla yapılabilmiştir. Böylece bu polinomlar için oldukça uzun bir liste elde edilmiştir. Bu çalışmada sadece $0 \leq n \leq 100$ için Dickson polinomlarının bir listesi verilmiştir.

Aşağıda Dickson polinomlarının hesabı MAPLE kullanılarak nasıl elde edildiği anlatılmaktadır.

MAPLE'da öncelikle Dickson polinomunun tanımı yapılmıştır. Daha sonra da $n \in \mathbb{N}$ için $D_n(x)$ polinomlarının hesabı için uygun döngü yazılarak algoritması verilmiştir. Böylece MAPLE ile istenen Dickson polinomlarının bir listesi elde edilir.

```
> Sum((-1)^i*n*(n-1-i)!/(n-2*i)!*1/i!*x^(n-2*i),i=0..floor(n/2));
```

$$\sum_{i=0}^{\mathrm{floor}\left(\frac{n}{2}\right)} \frac{(-1)^i\, n\, (n-1-i)!\, x^{(n-2\, i)}}{(n-2\, i)!\, i!}$$

```
> f:=proc(x)local n,D0;n:=0;D0:=1;for n from 1 to 100 do print(n,sort(sum((-1)^i*n*(n-1-i)!/(n-2*i)!*1/i!*x^(n-2*i),i=0..floor(n/2))));end do;end proc;
```

```
f := proc(x)
local n, D0;
    n := 0;
    D0 := 1;
    for n to 100 do print(n, sort( sum(
        (-1)^i×n×(n − 1 − i)!×x^(n − 2×i)/((n − 2×i)!×i!), i = 0 .. floor(1/2×n))))
    end do
end proc
```

```
> f(x);
```

$$n := 0$$
$$D0 := 1$$
$$1, x$$
$$2, x^2 - 2$$
$$3, x^3 - 3\,x$$
$$4, x^4 - 4\,x^2 + 2$$

$$5, x^5 - 5x^3 + 5x$$

$$6, x^6 - 6x^4 + 9x^2 - 2$$

$$7, x^7 - 7x^5 + 14x^3 - 7x$$

$$8, x^8 - 8x^6 + 20x^4 - 16x^2 + 2$$

$$9, x^9 - 9x^7 + 27x^5 - 30x^3 + 9x$$

$$10, x^{10} - 10x^8 + 35x^6 - 50x^4 + 25x^2 - 2$$

$$11, x^{11} - 11x^9 + 44x^7 - 77x^5 + 55x^3 - 11x$$

$$12, x^{12} - 12x^{10} + 54x^8 - 112x^6 + 105x^4 - 36x^2 + 2$$

$$13, x^{13} - 13x^{11} + 65x^9 - 156x^7 + 182x^5 - 91x^3 + 13x$$

$$14, x^{14} - 14x^{12} + 77x^{10} - 210x^8 + 294x^6 - 196x^4 + 49x^2 - 2$$

$$15, x^{15} - 15x^{13} + 90x^{11} - 275x^9 + 450x^7 - 378x^5 + 140x^3 - 15x$$

$$16, x^{16} - 16x^{14} + 104x^{12} - 352x^{10} + 660x^8 - 672x^6 + 336x^4 - 64x^2 + 2$$

$$17, x^{17} - 17x^{15} + 119x^{13} - 442x^{11} + 935x^9 - 1122x^7 + 714x^5 - 204x^3 + 17x$$

$$18, x^{18} - 18x^{16} + 135x^{14} - 546x^{12} + 1287x^{10} - 1782x^8 + 1386x^6 - 540x^4 + 81x^2 - 2$$

$$19, x^{19} - 19x^{17} + 152x^{15} - 665x^{13} + 1729x^{11} - 2717x^9 + 2508x^7 - 1254x^5 + 285x^3 - 19x$$

$$20, x^{20} - 20x^{18} + 170x^{16} - 800x^{14} + 2275x^{12} - 4004x^{10} + 4290x^8 - 2640x^6 + 825x^4 - 100x^2 + 2$$

$$\vdots$$

2.4. $\psi_n(x)$ Minimal Polinomları

$n \in \mathbb{N}$ olmak üzere $\mathbb{Q}$ üzerinde $x = cos\,2\pi/n$ 'nin minimal polinomu $\psi_n(x)$ ile gösterilsin. O halde $n = 2q$ için $\mathbb{Q}$ üzerinde $x = cos\,\pi/q$ 'nin minimal polinomu $\psi_{2q}(x)$ olur.

Aşağıda Watkins ve Zeitlin (1993) tarafından yapılan $deg\,\psi_n(x)$'in elde edilişi ile bilgiler verilecektir.

$\zeta_n = cos(2\pi/n) + i\,sin(2\pi/n)$ birimin n-inci ilkel kökü olsun.

$$cos(2\pi/n) = (\zeta_n + \zeta_n^{-1})/2$$

olduğundan $\mathbb{Q}$ rasyonel sayılar cismi üzerinde

$$\mathbb{Q}(\zeta_n) \supseteq \mathbb{Q}\big(cos(2\pi/n)\big) \supseteq \mathbb{Q}$$

bağıntısı geçerlidir. Buna göre $\mathbb{Q}$ üzerinde $\mathbb{Q}\big(cos(2\pi/n)\big)$ genişlemesinin derecesi hesaplanmalıdır. ζ_n,

$$x^2 - 2cos(2\pi/n)x + 1$$

ikinci dereceden polinomunun bir kökü olduğundan

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

ve

$$\big[\mathbb{Q}(\zeta_n) : \mathbb{Q}\big(cos(2\pi/n)\big)\big] = 1 \text{ veya } 2$$

eşitlikleri geçerli olur. Eğer $n \geq 3$ ise ζ_n reel değildir, dolayısı ile

$$\big[\mathbb{Q}(\zeta_n) : \mathbb{Q}\big(cos(2\pi/n)\big)\big] = 2$$

eşitliği geçerli olur. O halde

$$\big[\mathbb{Q}\big(cos(2\pi/n)\big) : \mathbb{Q}\big] = \varphi(n)/2$$

eşitliği bulunur. Böylece istenilen

$$\deg\ \psi_n(x) = \begin{cases} 1, & n = 1,2 \\ \varphi(n)/2\,, & n \geq 3 \end{cases}$$

eşitliği elde edilir.

Watkins ve Zeitlin (1993) tarafından verilen aşağıdaki teorem, Chebycheff polinomları yardımıyla $\psi_n(x)$ minimal polinomlarının hesabının nasıl yapıldığını açıklamaktadır.

Teorem 2.4.1. ψ_n, $\cos(2\pi/n)$'in minimal polinomu ve T_s, s-inci Chebycheff polinomu olmak üzere

i) $n = 2s + 1$ tek ise

$$T_{s+1}(x) - T_s(x) = 2^s \prod_{d|n} \psi_d(x)\,; \tag{2.3}$$

ii) $n = 2s$ çift ise

$$T_{s+1}(x) - T_{s-1}(x) = 2^s \prod_{d|n} \psi_d(x) \quad (2.4)$$

eşitlikleri geçerlidir.

İspat: Ayrıntılı ispat için Watkins ve Zeitlin (1993)'e bakınız.

Cangül (1993) çalışmasında $0 \leq n \leq 13$ için $\psi_n(x)$ minimal polinomların bir listesini vermiştir. Yine daha önce Chebycheff ve Dickson polinomlarında olduğu gibi bu $n \in \mathbb{N}$'nin artan değerleri için $\psi_n(x)$ minimal polinomlarının el ile hesaplanması oldukça zorlaşmakta ve zaman almaktadır. Bu amaçla bu tez çalışmasında bu polinomların hesabı Teorem 2.4.1. yardımıyla MAPLE kullanılarak yapılmış ve $n > 13$ için genişleyen bir liste kolaylıkla edilmiştir. Böylece $q > 50$ için λ_q 'nun minimal polinomlarının hesaplanması kolaylaşmıştır.

2.5. λ_q'nun minimal polinomu

Aşağıda λ_q'nun minimal polinomu ile ilgili bazı hatırlatmalar yapılacaktır.

$\lambda_q = 2cos\,(\pi/q)$'nun minimal polinomu P_q^* ile gösterilsin. Cangül (1993) çalışmasında deg P_q^* ile ilgili aşağıdaki teoremi ve sonucu vermiştir:

Teorem 2.5.1. P_q^* , $\lambda_q = 2cos\,(\pi/q)$'nun minimal polinomu olmak üzere

$$\deg P_q^* = \frac{\varphi(2q)}{2}$$

dir.

Teorem 2.5.1.'in ışığında q'nun tek ve çift olduğu durumlar için de aşağıdaki sonuç verilmiştir.

Sonuç 2.5.2. φ Euler fonksiyonu olsun. O zaman

$$\deg P_q^* = \begin{cases} \varphi(q)/2, & q \text{ tek ise} \\ \varphi(q), & q \text{ çift ise} \end{cases}$$

eşitliği geçerlidir.

Minimal polinomlar birim başkatsayılı olduğundan P_q^* ile ψ_{2q} minimal polinomları arasında

$$P_q^*(x) = 2^{\varphi(2q)/2}.\psi_{2q}(x/2)$$

bağıntısı geçerlidir.

q'nun tek ve çift olduğu durumlar için Cangül (1993) tarafından λ_q'nun $P_q^*(x)$ minimal polinomu aşağıdaki gibi verilmiştir:

Teorem 2.5.3. q tek olsun. O zaman λ_q'nun $P_q^*(x)$ minimal polinomu,

$$P_q^*(x) = 2^{\frac{\varphi(q)-q-1}{2}} . \frac{D_{\frac{q+1}{2}}(x) + D_{\frac{q-1}{2}}(x)}{\prod_{\substack{d|2q \\ d\neq 2q \\ d\, çift}} \psi_d(x/2)} \tag{2.5}$$

biçimindedir.

Örnek 2.5.4.

$q = 5$ için $\qquad P_5^*(x) = 2^{-1} . \frac{D_3(x)+D_2(x)}{\psi_2(x/2)}$

$$= x^2 - x - 1$$

$q = 15$ için $\qquad P_{15}^*(x) = 2^{-4} . \frac{D_8(x)+D_7(x)}{\psi_2(x/2)\psi_6(x/2)\psi_{10}(x/2)}$

$$= x^4 + x^3 - 4x^2 - 4x + 1.$$

Teorem 2.5.5. q çift olsun. O zaman λ_q'nun $P_q^*(x)$ mininimal polinomu,

$$P_q^*(x) = 2^{\frac{\varphi(2q)-q}{2}} . \frac{D_{q+1}(x) - D_{q-1}(x)}{\prod_{\substack{d|2q \\ d\neq 2q \\ d\nmid q}} \psi_d\left(\frac{x}{2}\right) . \left[D_{\frac{q}{2}+1}(x) - D_{\frac{q}{2}-1}(x)\right]} \tag{2.6}$$

biçimindedir.

Örnek 2.5.6.

$q = 4$ için $\qquad P_4^*(x) = \frac{D_5(x)-D_3(x)}{D_3(x)-D_1(x)}$

$$= x^2 - 2$$

$q = 10$ için $\qquad P_{10}^*(x) = 2^{-1} . \frac{D_{11}(x)-D_9(x)}{\psi_4(x).[D_6(x)-D_4(x)]}$

$$= x^4 - 5x^2 + 5$$

2.6. λ_q'nun Minimal Polinomunun Özellikleri

Bu bölümde P_q^* minimal polinomunun bazı özellikleri verilecektir. Daha sonra da P_q^* minimal polinomunun asal moddaki kökleri ile ilgili elde edilen sonuçlara değinilecektir. Aşağıdaki sonuç, Teorem 2.5.5'in özel bir hali olup q, ikinin kuvvetleri biçiminde olduğunda P_q^* minimal polinomunun elde edilişi ile bilgi vermektedir.

Sonuç 2.6.1. $q = 2^k$ $(k \geq 2)$ için $P_q^*(x)$ minimal polinomu,

$$P_{2^k}^*(x) = \frac{D_{2^k+1}(x) - D_{2^k-1}(x)}{D_{2^{k-1}+1}(x) - D_{2^{k-1}-1}(x)}$$

biçimindedir.

İspat. (2.6)'da $q = 2^k$ $(k \geq 2)$ için

$$P_{2^k}^*(x) = 2^{\frac{\varphi(2.2^k) - 2^k}{2}} \cdot \frac{D_{2^k+1}(x) - D_{2^k-1}(x)}{\prod_{\substack{d|2.2^k \\ d\neq 2.2^k \\ d\nmid 2^k}} \psi_d(x/2) \cdot \left[D_{\frac{2^k}{2}+1}(x) - D_{\frac{2^k}{2}-1}(x)\right]}$$

$$P_{2^k}^*(x) = 2^{\frac{\varphi(2^{k+1}) - 2^k}{2}} \cdot \frac{D_{2^k+1}(x) - D_{2^k-1}(x)}{\prod_{\substack{d|2^{k+1} \\ d\neq 2^{k+1} \\ d\nmid 2^k}} \psi_d(x/2) \cdot \left[D_{2^{k-1}+1}(x) - D_{2^{k-1}-1}(x)\right]} \tag{2.7}$$

eşitliği elde edilir. $2q = 2^{k+1}$, $d \neq 2^{k+1}$ ve $d \nmid 2^k$ iken $d|2^{k+1}$ olduğundan (2.7)'de

$$\prod_{\substack{d|2^{k+1} \\ d\neq 2^{k+1} \\ d\nmid 2^k}} \psi_d(x/2) = 1 \tag{2.8}$$

eşitliği alınır. (2.8) ve $\varphi(2^k) = 2^{k-1}$ (3.7)'de göz önüne alınırsa $P_q^*(x)$ minimal polinomu,

$$P_{2^k}^*(x) = \frac{D_{2^k+1}(x) - D_{2^k-1}(x)}{D_{2^{k-1}+1}(x) - D_{2^{k-1}-1}(x)}$$

istenilen biçime dönüşür.

Aşağıdaki teoremde q çift olduğunda P_q^* minimal polinomunun da çift olduğunu gösteriyoruz.

Teorem 2.6.2. $q \geq 3$ çift olsun. O zaman

$$P_q^*(x) = 2^{\frac{\varphi(2q)-q}{2}} \cdot \frac{D_{q+1}(x)-D_{q-1}(x)}{\prod_{\substack{d|2q \\ d\neq 2q \\ d\nmid q}} \psi_d\left(\frac{x}{2}\right) \cdot \left[D_{\frac{q}{2}+1}(x)-D_{\frac{q}{2}-1}(x)\right]}$$

minimal polinomu da çifttir.

İspat. $q \geq 3$ çift olsun. $P_q^*(-x) = P_q^*(x)$ olduğu gösterilmelidir.

q çift ise $q+1$ tek olur. Dolayısı ile

$$D_{q+1}(-x) = -D_{q+1}(x) \tag{2.9}$$

eşitliği alınır.

İki durum söz konusudur.

i) $q = 4k, k \in \mathbb{N}$ olsun. O zaman $x = -x$ için

$$P_q^*(-x) = 2^{\frac{\varphi(2q)-q}{2}} \cdot \frac{D_{q+1}(-x)-D_{q-1}(-x)}{\prod_{\substack{d|2q \\ d\neq 2q \\ d\nmid q}} \psi_d\left(-\frac{x}{2}\right) \cdot \left[D_{\frac{q}{2}+1}(-x)-D_{\frac{q}{2}-1}(-x)\right]} \tag{2.10}$$

minimal polinomu alınır.

$q = 4k$ için $\frac{q}{2}$ çift olur. Buradan da $\frac{q}{2}+1$ tek olarak elde edilir. Böylece

$$D_{\frac{q}{2}+1}(-x) = -D_{\frac{q}{2}+1}(x) \tag{2.11}$$

ve $q = 4k$ için

$$\prod_{\substack{d|8k \\ d\neq 8k \\ d\nmid 4k}} \psi_d(-x) = \prod_{\substack{d|8k \\ d\neq 8k \\ d\nmid 4k}} \psi_d(x) \tag{2.12}$$

eşitliği elde edilir. Böylece (2.9), (2.11) ve (2.12) eşitlikleri (2.10)'de göz önüne alınırsa

$$P_q^*(-x) = 2^{\frac{\varphi(2q)-q}{2}} \cdot \frac{-D_{q+1}(x)+D_{q-1}(x)}{\prod_{\substack{d|8k \\ d\neq 8k \\ d\nmid 4k}} \psi_d\left(-\frac{x}{2}\right) \cdot \left[-D_{\frac{q}{2}+1}(x) + D_{\frac{q}{2}+1}(x)\right]}$$

$$P_q^*(-x) = 2^{\frac{\varphi(2q)-q}{2}} \cdot \frac{(-1).\left[D_{q+1}(x)-D_{q+1}(x)\right]}{\prod_{\substack{d|8k \\ d\neq 8k \\ d\nmid 4k}} \psi_d\left(\frac{x}{2}\right).(-1)\left[D_{\frac{q}{2}+1}(x)- D_{\frac{q}{2}+1}(x)\right]}$$

$$P_q^*(-x) = 2^{\frac{\varphi(2q)-q}{2}}.\frac{D_{q+1}(x)-D_{q-1}(x)}{\prod_{\substack{d|2q \\ d\neq 2q \\ d\nmid q}} \psi_d\left(\frac{x}{2}\right).\left[D_{\frac{q}{2}+1}(x)- D_{\frac{q}{2}+1}(x)\right]} = P_q^*(x)$$

istenilen elde edilmiş olunur. Buradan da P_q^* çift minimal polinomdur.

ii) $q = 4k + 2$ ya da $q = 2k$, $k \in \mathbb{N}$ tek olsun. O zaman yine $x = -x$ için yine

$$P_q^*(-x) = 2^{\frac{\varphi(2q)-q}{2}}.\frac{D_{q+1}(-x)-D_{q-1}(-x)}{\prod_{\substack{d|2q \\ d\neq 2q \\ d\nmid q}} \psi_d\left(-\frac{x}{2}\right).\left[D_{\frac{q}{2}+1}(-x)-D_{\frac{q}{2}+1}(-x)\right]}$$

minimal polinomu alınır.

$q = 4k + 2$ ya da $q = 2k$, $k \in \mathbb{N}$ tek ise $\frac{q}{2}$ tek olur. Buradan da $\frac{q}{2} + 1$ çift için

$$D_{\frac{q}{2}+1}(-x) = D_{\frac{q}{2}+1}(x) \tag{2.13}$$

eşitliği elde edilir. $q = 2k$, k tek için

$$\prod_{\substack{d|4k \\ d\neq 4k \\ d\nmid 2k}} \psi_d(-x) = (-1).\prod_{\substack{d|4k \\ d\neq 4k \\ d\nmid 2k}} \psi_d(x) \tag{2.14}$$

eşitliği geçerli olur. Böylece yine (i) de olduğu gibi (2.9), (2.13) ve (2.14) eşitlikleri (2.10)'da ele alınırsa

$$P_q^*(-x) = 2^{\frac{\varphi(2q)-q}{2}}.\frac{- D_{q+1}(x)+ D_{q-1}(x)}{(-1).\prod_{\substack{d|4k \\ d\neq 4k \\ d\nmid 2k}} \psi_d\left(\frac{x}{2}\right).\left[D_{\frac{q}{2}+1}(x)-D_{\frac{q}{2}-1}(x)\right]}$$

$$P_q^*(-x) = 2^{\frac{\varphi(2q)-q}{2}}.\frac{(-1).[D_{q+1}(x)-D_{q-1}(x)]}{(-1).\prod_{\substack{d|4k \\ d\neq 4k \\ d\nmid 2k}} \psi_d\left(\frac{x}{2}\right).\left[D_{\frac{q}{2}+1}(x)-D_{\frac{q}{2}-1}(x)\right]}$$

$$P_q^*(-x) = 2^{\frac{\varphi(2q)-q}{2}}.\frac{D_{q+1}(x)- D_{q-1}(x)}{\prod_{\substack{d|2q \\ d\neq 2q \\ d\nmid q}} \psi_d\left(\frac{x}{2}\right).\left[D_{\frac{q}{2}+1}(x)-D_{\frac{q}{2}-1}(x)\right]} = P_q^*(x)$$

olur ve yine P_q^*'ın çift olduğu bulunur.

i) ve ii)'den P_q^* minimal polinomu çifttir.

2.7. Asal Modda Minimal Polinomun Kökleri

Bu bölümde $q \in \mathbb{Z}$, $q \geq 3$ olmak üzere $\mathbb{Q}$ üzerinde $\lambda_q = 2\cos \pi/q$'nun minimal polinomunun asal moddaki kökleri ile ilgili Ozgur ve arkadaşları (2011) tarafından elde edilen sonuçlardan bahsedilmiştir. Bu sonuçlar, Hecke Gruplarının denklik alt gruplarının hesaplanmasında yardımcı olacaktır.

Aşağıdaki teoremde q sayısının ikinin kuvvetleri biçiminde olması durumunda minimal polinomun mod 2'de sıfır köküne sahip olduğunu belirtiyoruz.

Teorem 2.7.1. (Ozgur ve ark. 2011c) $q \geq 3$ ve $q = 2^k (k \geq 2)$, $k \in \mathbb{Z}$ olmak üzere $x = 0, mod$ 2'ye göre $P^*_{2^k}(x)$'in kökücür.

Teorem 2.7.1'in ispatına geçilmeden önce bu teoremin alt yapısını oluşturan bazı yardımcı teoremleri ispatları ile birlikte veriyoruz.

Yardımcı Teorem 2.7.1.a. $q \geq 3$ ve $q = 2^k$ $(k \geq 2)$, $k \in \mathbb{Z}$ ve A bir sabit olmak üzere $P^*_{2^k}(x)$ minimal polinomun payı

$$D_{2^k+1}(x) - D_{2^k-1}(x) = x[2^{k+1} + \sum Ax]$$

biçimindedir, burada

$$\sum Ax = \left[(-1)^{2^{k-1}-1} \tfrac{2^k+1}{2^k-2^{k-1}} \binom{2^k - 2^{k-1}}{2^{k-1} - 1} x^2 + \cdots + (-1)^1 \tfrac{2^k+1}{2^k} \binom{2^k}{1} x^{2^k-2} + x^{2^k}\right.$$

$$\left. - \left[(-1)^{2^{k-1}-2} \tfrac{2^k-1}{2^k-2^{k-1}+1} \binom{2^k - 2^{k-1} + 1}{2^{k-1} - 2} x^2 + \ldots + (-1)^1 \tfrac{2^k-1}{2^k-2} \binom{2^k - 2}{1} x^{2^k-4} + x^{2^k-2}\right]\right.$$

dir.

İspat. $q \geq 3$ ve $q = 2^k$ $(k \geq 2)$, $k \in \mathbb{Z}$ için Sonuç 2.6.1'den $P^*_{2^k}$ minimal polinomunun payı

$$D_{2^k+1}(x) - D_{2^k-1}(x) \tag{2.15}$$

şeklindedir.

(2.2)'deki Dickson polinomlarının tanımı (2.15) için kullanılırsa

$$D_{2^k+1}(x) = \sum_{i=0}^{\left[\frac{2^k+1}{2}\right]} (-1)^i \tfrac{2^k+1}{2^k+1-i} \binom{2^k + 1 - i}{i} x^{2^k+1-2i}$$

ve

$$D_{2^k-1}(x) = \sum_{i=0}^{\left[\frac{2^k-1}{2}\right]} (-1)^i \frac{2^k-1}{2^k-1-i} \binom{2^k-1-i}{i} x^{2^k-1-2i}$$

eşitlikleri geçerli olur. Böylece istenilen $D_{2^k+1}(x) - D_{2^k-1}(x)$ farkı için

$$D_{2^k+1}(x) - D_{2^k-1}(x) = \sum_{i=0}^{\left[2^{k-1}+\frac{1}{2}\right]} (-1)^i \frac{2^k+1}{2^k+1-i} \binom{2^k+1-2i}{i} x^{2^k+1-2i} \quad (2.16)$$
$$- \sum_{i=0}^{\left[2^{k-1}-\frac{1}{2}\right]} (-1)^i \frac{2^k-1}{2^k-1-i} \binom{2^k-1-i}{i} x^{2^k-1-2i}$$

eşitliği alınır. (2.16)'da gerekli düzenlemelerden sonra

$$D_{2^k+1}(x) - D_{2^k-1}(x) = \sum_{i=0}^{2^{k-1}} (-1)^i \frac{2^k+1}{2^k+1-i} \binom{2^k+1-i}{i} x^{2^k+1-2i} \quad (2.17)$$
$$- \sum_{i=0}^{2^{k-1}-1} (-1)^i \frac{2^k-1}{2^k-1-i} \binom{2^k-1-i}{i} x^{2^k-1-2i}$$

eşitliği elde edilir. (2.17)'de toplam sembolü altındaki terimler açıldığında

$$D_{2^k+1}(x) - D_{2^k-1}(x) = (-1)^{2^{k-1}} \frac{2^k+1}{2^k+1-2^{k-1}} \binom{2^k+1-2^{k-1}}{2^{k-1}} x^{2^k+1-2^k} \quad (2.18)$$
$$+(-1)^{2^{k-1}-1} \frac{2^k+1}{2^k+1-2^{k-1}-1} \binom{2^k+1-2^{k-1}-1}{2^{k-1}-1} x^{2^k+1-2^k-2} + \cdots +$$
$$+(-1)^1 \frac{2^k+1}{2^k+1-1} \binom{2^k+1-1}{1} x^{2^k+1-2} + (-1)^0 \frac{2^k+1}{2^k+1} \binom{2^k+1}{0} x^{2^k+1}$$
$$-\Big[(-1)^{2^{k-1}-1} \frac{2^k-1}{2^{k-1}-2^{k-1}+1} \binom{2^{k-1}-2^{k-1}+1}{2^{k-1}-1} x^{2^k-1-2^k+2}$$
$$+(-1)^{2^{k-1}-2} \frac{2^k-1}{2^k-1-2^{k-1}+2} \binom{2^k-1-2^{k-1}+2}{2^{k-1}-2} x^{2^k-1-2^k+4} + \cdots$$
$$+(-1)^1 \frac{2^k-1}{2^k-1-1} \binom{2^k-1-1}{1} x^{2^k-1-2} + (-1)^0 \frac{2^k-1}{2^k-1} \binom{2^k-1}{0} x^{2^k-1}\Big]$$

eşitliği alınır. (2.18) eşitliğinin düzenlenmesi sonucunda

$$D_{2^k+1}(x) - D_{2^k-1}(x) = (-1)^{2^{k-1}} \frac{2^k+1}{2^k+1-2^{k-1}} \binom{2^k+1-2^{k-1}}{2^{k-1}} x \quad (2.19)$$
$$+(-1)^{2^{k-1}-1} \frac{2^k+1}{2^k-2^{k-1}} \binom{2^k-2^{k-1}}{2^{k-1}-1} x^3 + \cdots + (-1)^1 \frac{2^k+1}{2^k} \binom{2^k}{1} x^{2^k-1}$$
$$+x^{2^k+1} - \Big[(-1)^{2^{k-1}-1} \frac{2^k-1}{2^{k-1}-2^{k-1}+1} \binom{2^{k-1}-2^{k-1}+1}{2^{k-1}-1} x$$

$$+(-1)^{2^{k-1}-2}\frac{2^k-1}{2^k-2^{k-1}+1}\binom{2^k-2^{k-1}+1}{2^{k-1}-2}x^3+\cdots$$

$$+(-1)^1\frac{2^k-1}{2^k-2}\binom{2^k-2}{1}x^{2^k-3}+x^{2^k-1}\Big]$$

eşitliği elde edilir. Dikkat edilirse (2.19) eşitliğinde her bir terim x bilinmeyenini içerir. Dolayısı ile bu eşitlik x parantezine alınırsa

$$D_{2^k+1}(x)-D_{2^k-1}(x)=x\Big[(-1)^{2^{k-1}}\frac{2^k+1}{2^k+1-2^{k-1}}\binom{2^k+1-2^{k-1}}{2^{k-1}} \tag{2.20}$$

$$+(-1)^{2^{k-1}-1}\frac{2^k+1}{2^k-2^{k-1}}\binom{2^k-2^{k-1}}{2^{k-1}-1}x^2+\cdots+(-1)^1\frac{2^k+1}{2^k}\binom{2^k}{1}x^{2^k-2}$$

$$+x^{2^k}-\Big[(-1)^{2^{k-1}-1}\frac{2^k-1}{2^k-1-2^{k-1}+1}\binom{2^k-1-2^{k-1}+1}{2^{k-1}-1}$$

$$+(-1)^{2^{k-1}-2}\frac{2^k-1}{2^k-2^{k-1}+1}\binom{2^k-2^{k-1}+1}{2^{k-1}-2}x^3+\cdots$$

$$+(-1)^1\frac{2^k-1}{2^k-2}\binom{2^k-2}{1}x^{2^k-3}+x^{2^k-1}\Big]\Big]$$

eşitliği alınır. Böylece (2.20) eşitliğinde son düzenlemelerin yapılması ile minimal polinomun payı için istenilen

$$D_{2^k+1}(x)-D_{2^k-1}(x)=x\Big[\frac{2^k+1}{2^k+1-2^{k-1}}.(2^k+1-2^{k-1})+$$

$$+(-1)^{2^{k-1}-1}\frac{2^k+1}{2^k-2^{k-1}}\binom{2^k-2^{k-1}}{2^{k-1}-1}x^2+\cdots+(-1)^1\frac{2^k+1}{2^k}\binom{2^k}{1}x^{2^k-2}$$

$$+x^{2^k}-\Big[-\frac{2^k-1}{2^{k-1}-2^{k-2}}.(2^{k-1}-2^{k-2})+$$

$$+(-1)^{2^{k-1}-2}\frac{2^k-1}{2^k-2^{k-1}+1}\binom{2^k-2^{k-1}+1}{2^{k-1}-2}x^2+\cdots$$

$$+(-1)^1\frac{2^k-1}{2^k-2}\binom{2^k-2}{1}x^{2^k-4}+x^{2^k-2}\Big]\Big]$$

$$D_{2^k+1}(x)-D_{2^k-1}(x)=x[2^k+1+2^k-1+\sum Ax]$$

$$D_{2^k+1}(x)-D_{2^k-1}(x)=x[2^{k+1}+\sum Ax]$$

eşitliği bulunur.

Yardımcı Teorem 2.7.1.b. $q \geq 3$ ve $q = 2^k$ $(k \geq 2)$, $k \in \mathbb{Z}$ ve B bir sabit olmak üzere $P^*_{2^k}(x)$ minimal polinomun paydası,

$$D_{2^{k-1}+1}(x) - D_{2^{k-1}-1}(x) = x[2^k + \sum Bx]$$

biçimindedir, burada

$$\sum Bx = \Bigg[(-1)^{2^{k-2}-1} \tfrac{2^{k-1}+1}{2^{k-1}-2^{k-2}+2} \binom{2^{k-1}-2^{k-2}+2}{2^{k-2}-1} x^2 + \cdots$$

$$+(-1)^1 \tfrac{2^{k-1}+1}{2^{k-1}} \binom{2^{k-1}}{1} x^{2^{k-1}-2} + x^{2^{k-1}}$$

$$-\Bigg[(-1)^{2^{k-2}-2} \frac{2^{k-1}-1}{2^{k-1}-2^{k-2}+1} \binom{2^{k-1}-2^{k-2}+1}{2^{k-2}-2} x^2 + \cdots$$

$$+(-1)^1 \tfrac{2^{k-1}-1}{2^{k-1}-2} \binom{2^{k-1}-2}{1} x^{2^{k-1}-4} + x^{2^{k-1}-2}\Bigg]\Bigg]$$

dir.

İspat. $q \geq 3$ ve $q = 2^k$ $(k \geq 2)$, $k \in \mathbb{Z}$ için Sonuç 2.6.1'den $P^*_{2^k}$ minimal polinomunun paydası

$$D_{2^{k-1}+1}(x) - D_{2^{k-1}-1}(x) \tag{2.21}$$

şeklindedir.

Yardımcı Teorem 2.7.1.a'dakine benzer olarak (2.2)'deki Dickson polinomlarının tanımı (2.21)'de göz önünde bulundurulursa

$$D_{2^{k-1}+1}(x) = \sum_{i=0}^{\left[\frac{2^{k-1}+1}{2}\right]} (-1)^i \tfrac{2^{k-1}+1}{2^{k-1}+1-i} \binom{2^{k-1}+1-i}{i} x^{2^{k-1}+1-2i}$$

ve

$$D_{2^{k-1}-1}(x) = \sum_{i=0}^{\left[\frac{2^{k-1}-1}{2}\right]} (-1)^i \tfrac{2^{k-1}-1}{2^{k-1}-1-i} \binom{2^{k-1}-1-i}{i} x^{2^{k-1}-1-2i}$$

eşitlikleri alınır. Böylece istenilen $D_{2^{k-1}+1}(x) - D_{2^{k-1}-1}(x)$ farkı için

$$D_{2^{k-1}+1}(x) - D_{2^{k-1}-1}(x) = \sum_{i=0}^{\left[2^{k-2}+\frac{1}{2}\right]} (-1)^i \frac{2^{k-1}+1}{2^{k-1}+1-i} \binom{2^{k-1}+1-i}{i} x^{2^{k-1}+1-2i}$$

$$- \sum_{i=0}^{\left[2^{k-2}-\frac{1}{2}\right]} (-1)^i \frac{2^{k-1}-1}{2^{k-1}-1-i} \binom{2^{k-1}-1-i}{i} x^{2^{k-1}-1-2i}$$

eşitliği geçerli olur. Minimal polinomun payda kısmında istenileni elde etmek için yukarıdaki eşitlikte gerekli düzenlemeler yapıldığında

$$D_{2^k+1}(x) - D_{2^k-1}(x) = \sum_{i=0}^{2^{k-2}} (-1)^i \frac{2^{k-1}+1}{2^{k-1}+1-i} \binom{2^{k-1}+1-i}{i} x^{2^{k-1}+1-2i} \tag{2.22}$$

$$- \sum_{i=0}^{2^{k-2}-1} (-1)^i \frac{2^{k-1}-1}{2^{k-1}-1-i} \binom{2^{k-1}-1-i}{i} x^{2^{k-1}-1-2i}$$

eşitliği bulunur. (2.22)'de toplam sembolü altındaki terimlerin açılması ile

$$D_{2^{k-1}+1}(x) - D_{2^{k-1}-1}(x) = \tag{2.23}$$

$$= (-1)^{2^{k-2}} \frac{2^{k-1}+1}{2^{k-1}+1-2^{k-2}} \binom{2^{k-1}+1-2^{k-2}}{2^{k-1}} x^{2^{k-1}+1-2^{k-1}}$$

$$+(-1)^{2^{k-2}-1} \frac{2^{k-1}+1}{2^{k-1}+1-2^{k-2}-1} \binom{2^{k-1}+1-2^{k-2}-1}{2^{k-2}-1} x^{2^{k-1}+1-2^{k-1}+2} + \cdots$$

$$+(-1)^1 \frac{2^{k-1}+1}{2^{k-1}+1-1} \binom{2^{k-1}+1-1}{1} x^{2^k+1-2} + (-1)^0 \frac{2^{k-1}+1}{2^{k-1}+1} \binom{2^{k-1}+1}{0} x^{2^{k-1}+1}$$

$$-\Big[(-1)^{2^{k-2}-1} \frac{2^{k-1}-1}{2^{k-1}-2^{k-2}+1} \binom{2^{k-1}-1-2^{k-2}+1}{2^{k-2}-1} x^{2^{k-1}-1-2^{k-1}+2}$$

$$+(-1)^{2^{k-2}-1} \frac{2^{k-1}-1}{2^{k-1}-1-2^{k-2}+2} \binom{2^{k-1}-1-2^{k-2}+2}{2^{k-2}-2} x^{2^{k-1}-1-2^{k-1}+4} + \cdots$$

$$+(-1)^1 \frac{2^{k-1}-1}{2^{k-1}-1-1} \binom{2^{k-1}-1-1}{1} x^{2^{k-1}-1-2} + (-1)^0 \frac{2^{k-1}-1}{2^{k-1}-1} \binom{2^{k-1}-1}{0} x^{2^{k-1}-1}\Big]$$

eşitliği alınır. (2.23)'de yapılan gerekli düzenlemeler sonucu

$$D_{2^{k-1}+1}(x) - D_{2^{k-1}-1}(x) = (-1)^{2^{k-2}} \frac{2^{k-1}+1}{2^{k-1}+1-2^{k-2}} \binom{2^{k-1}+1-2^{k-2}}{2^{k-2}} x \tag{2.24}$$

$$+(-1)^{2^{k-2}-2} \frac{2^{k-1}+1}{2^{k-1}-2^{k-2}} \binom{2^{k-1}-2^{k-2}}{2^{k-2}-1} x^3$$

$$+\cdots+(-1)^{1}\frac{2^{k-1}+1}{2^{k-1}}\binom{2^{k-1}}{1}x^{2^{k-1}-1}++x^{2^{k-1}+1}++x^{2^{k-1}+1}$$

$$-\Big[(-1)^{2^{k-2}-1}\frac{2^{k-1}-1}{2^{k-1}-2^{k-2}}\binom{2^{k-1}-2^{k-2}}{2^{k-1}-1}x$$

$$+(-1)^{2^{k-2}-2}\frac{2^{k-1}-1}{2^{k-1}-2^{k-2}+1}\binom{2^{k-1}-2^{k-2}+1}{2^{k-2}-2}x^{3}+\cdots$$

$$+(-1)^{1}\frac{2^{k-1}-1}{2^{k-1}-2}\binom{2^{k-1}-2}{1}x^{2^{k-1}-3}+x^{2^{k-1}-1}\Big]$$

eşitliği bulunur. Yardımcı Teorem 2.7.1.a' ya benzer olarak (2.24) eşitliği x parantezine alınırsa

$$D_{2^{k-1}+1}(x)-D_{2^{k-1}-1}(x)=x\Big[(-1)^{2^{k-2}}\frac{2^{k-1}+1}{2^{k-1}+1-2^{k-2}}.(2^{k-1}+1-2^{k-2})$$

$$+(-1)^{2^{k-2}-1}\frac{2^{k-1}+1}{2^{k-1}-2^{k-2}+2}\binom{2^{k-1}-2^{k-2}+2}{2^{k-2}-1}x^{2}+\cdots$$

$$+(-1)^{1}\frac{2^{k-1}+1}{2^{k-1}}\binom{2^{k-1}}{1}x^{2^{k-1}-2}+x^{2^{k-1}}$$

$$-\Big[(-1)^{2^{k-2}-1}\frac{2^{k-1}-1}{2^{k-1}-2^{k-2}}.(2^{k-1}-2^{k-2})$$

$$+(-1)^{2^{k-2}-2}\frac{2^{k-1}-1}{2^{k-1}-2^{k-2}+1}\binom{2^{k-1}-2^{k-2}+1}{2^{k-2}-2}x^{2}+\cdots$$

$$+(-1)^{1}\frac{2^{k-1}-1}{2^{k-1}-2}\binom{2^{k-1}-2}{1}x^{2^{k-1}-4}+x^{2^{k-1}-2}\Big]\Big]$$

$$D_{2^{k-1}+1}(x)-D_{2^{k-1}-1}(x)=x[2^{k-1}+1+2^{k-1}-1+\sum Bx]$$

$$D_{2^{k-1}+1}(x)-D_{2^{k-1}-1}(x)=x[2.2^{k-1}+\sum Bx]$$

$$D_{2^{k-1}+1}(x)-D_{2^{k-1}-1}(x)=x[2^{k}+\sum Bx]$$

eşitliği bulunur ki bu da minimal polinomun paydası için istenilen eşitliktir.

Yardımcı Teorem 2.7.1.a ve 2.7.1.b'nin verilmesinden sonra Teorem 2.7.1'in ispatına geçebiliriz.

İspat: $q \geq 3$ ve $q = 2^k$ $(k \geq 2)$, $k \in \mathbb{Z}$ olsun. $x = 0$ için $P^*_{2^k}(x) \equiv 0 \ mod\ 2$ olduğu gösterilmelidir.

$q = 2^k$ için Teorem 2.6.2 gereğince $P^*_{2^k}$ minimal polinomu da çifttir. Sonuç 2.6.1'e göre de minimal polinom

$$q = 2^k \text{ için} \qquad P^*_{2^k}(x) = \frac{D_{2^k+1}(x) - D_{2^k-1}(x)}{D_{2^{k-1}+1}(x) - D_{2^{k-1}-1}(x)} \tag{2.25}$$

biçimindedir. Buradan da $P^*_{2^k}$ minimal polinomun payı için Yardımcı Teorem 2.7.1.a ve paydası için de Yardımcı Teorem 2.7.1.b kullanılırsa $P^*_{2^k}$ minimal polinomu için

$$P^*_{2^k}(x) = \frac{x\left(2^{k+1} + \sum Ax\right)}{x\left(2^k + \sum Bx\right)} \tag{2.26}$$

eşitliği geçerli olur. Böylece (2.26) eşitliği ile minimal polinomun $x = 0$ için mod 2'de neye denk olduğu bulunabilir. Buna göre

$$x = 0 \text{ için} \qquad P^*_{2^k}(0) = \frac{2^{k+1} + \sum A.0}{2^k + \sum B.0}$$

$$P^*_{2^k}(0) = \frac{2^{k+1}}{2^k}$$

$$P^*_{2^k}(0) = 2 \tag{2.27}$$

eşitliği alınır. (2.27)'den de moda geçildiğinde istenilen

$$P^*_{2^k}(0) \equiv 0 \ \ mod\ 2$$

denkliği elde edilir. O halde $x = 0$, $P^*_{2^k}$ minimal polinomun mod 2'de bir köküdür.

Minimal polinomun $mod\ p$'de sıfır köküne sahip olduğuna ilişkin diğer bir sonucu da aşağıdaki teorem ile veriyoruz.

Teorem 2.7.2. (Ozgur ve ark. 2011c) $p > 2$ asal sayı olmak üzere $q = 2p$ iken $x = 0$, $mod\ p$'ye göre $P^*_{2p}(x)$'in bir köküdür.

Yukarıda Teorem 2.7.1'de olduğu gibi benzer olarak yine bu teoremin ispatını kolaylaştıracak bazı yardımcı teoremler ispatları ile birlikte verilecektir. Öncelikle $q = 2p$ durumundaki minimal polinom bulunmalıdır.

Aşağıdaki yardımcı teoremde q'nun bir asalın iki katı olması durumundaki minimal polinomun ne olduğunu veriyoruz.

Yardımcı Teorem 2.7.2.a. $q \geq 3$, $p > 2$ asal olmak üzere $q = 2p$ iken $P_q^*(x)$ minimal polinomu,

$$P_{2p}^*(x) = 2^{-1}.\frac{D_{2p+1}(x)+D_{2p-1}(x)}{\prod_{\substack{d|4p \\ d\neq 4p \\ d\nmid 2p}} \psi_d\left(\frac{x}{2}\right).\left[D_{p+1}(x)-D_{p-1}(x)\right]} \tag{2.28}$$

şeklindedir.

İspat. $q \geq 3$, $p > 2$ asal olsun.

$q = 2p$ çift iken Teorem 2.6.2 gereğince P_{2p}^* minimal polinomu da çifttir. Buna göre

$$q = 2p \text{ için} \qquad P_{2p}^*(x) = 2^{\frac{\varphi(2\cdot 2p)-2p}{2}}.\frac{D_{2p+1}(x)-D_{2p-1}(x)}{\prod_{\substack{d|2.2p \\ d\neq 2.2p \\ d\nmid 2p}} \psi_d\left(\frac{x}{2}\right).\left[D_{\frac{2p}{2}+1}(x)-D_{\frac{2p}{2}-1}(x)\right]}$$

$$P_{2p}^*(x) = 2^{\frac{\varphi(4p)-2p}{2}}.\frac{D_{2p+1}(x)-D_{2p-1}(x)}{\prod_{\substack{d|4p \\ d\neq 4p \\ d\nmid 2p}} \psi_d\left(\frac{x}{2}\right).\left[D_{p+1}(x)-D_{p-1}(x)\right]} \tag{2.29}$$

eşitliği alınır. (2.29) eşitliğinde φ Euler fonksiyonu olmak üzere

$$\varphi(4p) = \varphi(4).\varphi(p) = 2(p-1) = 2p-2$$

olduğu göz önüne alınırsa böylece istenilen minimal polinom

$$P_{2p}^*(x) = 2^{-1}.\frac{D_{2p+1}(x)-D_{2p-1}(x)}{\prod_{\substack{d|4p \\ d\neq 4p \\ d\nmid 2p}} \psi_d\left(\frac{x}{2}\right).\left[D_{p+1}(x)-D_{p-1}(x)\right]}$$

biçiminde bulunur.

(2.28) eşitliğindeki minimal polinomda çarpım sembolü altındaki ifadenin belirli koşullar altında neye eşit olduğunu aşağıdaki yardımcı teoremde belirtiyoruz.

Yardımcı Teorem 2.7.2.b. $p > 2$ asal olmak üzere

$$\prod_{\substack{d|4p \\ d\neq 4p \\ d\nmid 2p}} \psi_d\left(\frac{x}{2}\right) = \frac{x}{2}$$

eşitliği geçerlidir.

İspat. $p > 2$ asal olsun. O zaman $d|4p, d \neq 4p, d \nmid 2p$ koşulları altında d'nin bölenleri: $1, 2, 4, p, 2p, 4p$'dir. Verilen koşullara uyan d'nin bir tek böleni 4'tür. Buna göre

$$\prod_{\substack{d|4p \\ d\neq 4p \\ d\nmid 2p}} \psi_d\left(\frac{x}{2}\right) = \psi_4\left(\frac{x}{2}\right) \tag{2.30}$$

eşitliği elde edilir. (2.30)'da $\psi_4\left(\frac{x}{2}\right)$ minimal polinomu

$$\frac{x}{2} = cos\frac{2\pi}{4} = \cos\frac{\pi}{2} = 0 \tag{2.31}$$

olarak bulunur. (2.31)'in (2.30) eşitliğinde ele alınması ile istenilen eşitlik

$$\prod_{\substack{d|4p \\ d\neq 4p \\ d\nmid 2p}} \psi_d\left(\frac{x}{2}\right) = \psi_4\left(\frac{x}{2}\right) = \frac{x}{2}$$

biçiminde bulunur.

Aşağıdaki yardımcı teoremde minimal polinomun payı ile ilgili bilgi veriyoruz.

Yardımcı Teorem 2.7.2.c. $p > 2$ asal ve A bir sabit olmak üzere P_{2p}^* minimal polinomunun payı,

$$D_{2p+1}(x) - D_{2p-1}(x) = x(-4p + \sum Ax)$$

biçimindedir, burada $\sum Ax = \left[(-1)^{p-1}\frac{2p+1}{p+2}\binom{p+2}{p-1}x^2 + \cdots + (-1)^1(2p+1)x^{2p-2}\right.$ $\left.+x^{2p} - \left[(-1)^{p-2}\frac{2p-1}{p+1}\binom{p+1}{p-2}x^2 + \cdots + (-1)^1(2p-1)x^{2p-4} + x^{2p-2}\right]\right.$'dir.

İspat. $p > 2$ asal olsun. (2.2)'deki Dickson polinomlarının tanımından

$$D_{2p+1}(x) = \sum_{i=0}^{\left[\frac{2p+1}{2}\right]}(-1)^i\frac{2p+1}{2p+1-i}\binom{2p+1-i}{i}x^{2p+1-2i} \tag{2.32}$$

ve

$$D_{2p-1}(x) = \sum_{i=0}^{\left[\frac{2p-1}{2}\right]} (-1)^i \frac{2p-1}{2p-1-i} \binom{2p-1-i}{i} x^{2p-1-2i} \tag{2.33}$$

eşitlikleri alınır. (2.32) ve (2.33) eşitliklerinde gerekli düzenlemeler yapıldığında

$$D_{2p+1}(x) = \sum_{i=0}^{p} (-1)^i \frac{2p+1}{2p+1-i} \binom{2p+1-i}{i} x^{2p+1-2i}$$

ve

$$D_{2p-1}(x) = \sum_{i=0}^{p-1} (-1)^i \frac{2p-1}{2p-1-i} \binom{2p-1-i}{i} x^{2p-1-2i}$$

eşitlikleri elde edilir. Pay için istenilen $D_{2p+1}(x) - D_{2p-1}(x)$ farkı alınıp toplam sembolü altındaki terimler açılırsa

$$\begin{aligned} D_{2p+1}(x) - D_{2p-1}(x) =& (-1)^p \frac{2p+1}{p+1} \binom{p+1}{p} x + (-1)^{p-1} \frac{2p+1}{p+2} \binom{p+2}{p-1} x^3 + \cdots \\ &+(-1)^1 \frac{2p+1}{2p} \binom{2p}{1} x^{2p-1} + (-1)^0 \frac{2p+1}{2p+1} \binom{2p}{0} x^{2p+1} \\ &-\Big[(-1)^{p-1} \frac{2p-1}{p} \binom{p}{p-1} x + (-1)^{p-2} \frac{2p-1}{p+1} \binom{p+1}{p-2} x^3 + \cdots \\ &+(-1)^1 \frac{2p-1}{2p-2} \binom{2p-2}{1} x^{2p-3} + (-1)^0 \frac{2p-1}{2p-1} \binom{p-1}{0} x^{2p-1}\Big] \end{aligned} \tag{2.34}$$

eşitliği alınır. (2.34)'te gerekli hesaplamaların yapılması ile

$$\begin{aligned} D_{2p+1}(x) - D_{2p-1}(x) =& (-1)^p (2p+1)x + (-1)^{p-1} \frac{2p+1}{p+2} \binom{p+2}{p-1} x^3 + \cdots \\ &+(-1)^1 (2p+1) x^{2p-1} + x^{2p+1} \\ &-\Big[(-1)^{p-1} (2p-1)x + (-1)^{p-2} \frac{2p-1}{p+1} \binom{p+1}{p-2} x^3 + \cdots \\ &+(-1)^1 (2p-1) x^{2p-3} + x^{2p-1}\Big] \end{aligned} \tag{2.35}$$

eşitliği elde edilir. (2.35) eşitliği x parantezine alınırsa istenilen $D_{2p+1}(x) - D_{2p-1}(x)$ farkı

$$D_{2p+1}(x) - D_{2p-1}(x) = x\Big[(-1)^p(2p+1) + (-1)^{p-1}\tfrac{2p+1}{p+2}\binom{p+2}{p-1}x^2 + \cdots \qquad (2.36)$$

$$+(-1)^1(2p+1)x^{2p-2} + x^{2p}$$

$$-\Big[(-1)^{p-1}(2p-1) + (-1)^{p-2}\tfrac{2p-1}{p+1}\binom{p+1}{p-2}x^2 + \cdots$$

$$+(-1)^1(2p-1)x^{2p-4} + x^{2p-2}\Big]$$

şeklinde elde edilir. Böylece (2.36)'da gerekli düzenlemeler yapıldığında minimal polinomun payı için istenilen fark

$$D_{2p+1}(x) - D_{2p-1}(x) = x[(-1)^p(2p+1) - (-1)^{p-1}(2p-1) + \textstyle\sum Ax]$$

$$D_{2p+1}(x) - D_{2p-1}(x) = x[-(2p+1) - (2p-1) + \textstyle\sum Ax]$$

$$D_{2p+1}(x) - D_{2p-1}(x) = x[-2p - 1 - 2p + 1 + \textstyle\sum Ax]$$

$$D_{2p+1}(x) - D_{2p-1}(x) = x[-4p + \textstyle\sum Ax]$$

eşitliğine dönüşür.

Minimal polinomun paydasına ilişkin gerekli bilgiyi aşağıdaki yardımcı teorem ile veriyoruz.

Yardımcı Teorem 2.7.2.d. $p > 2$ asal ve B bir sabit olmak üzere P_{2p}^* minimal polinomunun paydası,

$$D_{2p+1}(x) - D_{2p-1}(x) = (-1)^{\frac{p+1}{2}}.4 + \textstyle\sum Bx$$

biçimindedir. Burada $\sum Bx = [x^{2k} - \frac{2k}{2k-1}\binom{2k-1}{1}x^{2k-2} + \cdots + \frac{2k}{k+1}\binom{k+1}{k-1}x^2$
$-(x^{2k-2} + \cdots + (-1)^{k-2}\frac{2k-2}{k}\binom{k}{k-2}x^2)\Big]$'dir.

İspat. $p > 2$ asal olsun. Pay kısmındakine benzer olarak (2.2)'deki Dickson polinomlarının tanımından

$$D_{p+1}(x) = \sum_{i=0}^{\left[\frac{p+1}{2}\right]}(-1)^i\frac{p+1}{p+1-i}\binom{p+1-i}{i}x^{p+1-2i} \qquad (2.37)$$

ve

$$D_{p-1}(x) = \sum_{i=0}^{\left[\frac{p-1}{2}\right]} (-1)^i \frac{p-1}{p-1-i} \binom{p-1-i}{i} x^{p-1-2i} \tag{2.38}$$

eşitlikleri alınır. (2.37) ve (2.38) eşitliklerinde toplam sembollerinin üst indisleri arasında $\frac{p+1}{2} = k,\ k \in \mathbb{Z}$ olmak üzere

$$p = 2k - 1 \text{ için} \qquad \left[\frac{p+1}{2}\right] = 1 + \left[\frac{p-1}{2}\right] \tag{2.39}$$

ilişkisinin olduğu görülür. Bu sebeple (2.37) ve (2.38) eşitlikleri,

$$D_{2k}(x) = \sum_{i=0}^{k} (-1)^i \frac{2k}{2k-i} \binom{2k-i}{i} x^{2k-2i}$$

ve

$$D_{2k-2}(x) = \sum_{i=0}^{k-1} (-1)^i \frac{2k-2}{2k-2-i} \binom{2k-2-i}{i} x^{2k-2-2i}$$

eşitliklerine dönüşür. Böylece minimal polinomun paydası için istenilen $D_{2k}(x) - D_{2k-2}(x)$ farkı

$$D_{2k}(x) - D_{2k-2}(x) = (-1)^k \frac{2k}{2k-k} \binom{2k-k}{k} \tag{2.40}$$

$$+ \sum_{i=0}^{k-1} (-1)^i \frac{2k}{2k-i} \binom{2k-i}{i} x^{2k-2i} - \sum_{i=0}^{k-1} (-1)^i \frac{2k-2}{2k-2-i} \binom{2k-2-i}{i} x^{2k-2-i}$$

olarak bulunur. (2.40)'ta toplam sembollerinin üst indisleri eşit olduğundan bu toplamlar, tek toplam altında toplandığında istenilen $D_{2k}(x) - D_{2k-2}(x)$ farkı

$$D_{2k}(x) - D_{2k-2}(x) = (-1)^k \frac{2k}{2k-k} \binom{2k-k}{k} x^{2k-2k} \tag{2.41}$$

$$+ \sum_{i=0}^{k-1} (-1)^i \left[\frac{2k}{2k-i} \binom{2k-i}{i} x^{2k-2i} - \frac{2k-2}{2k-2-i} \binom{2k-2-i}{i} x^{2k-2-2i}\right]$$

şeklinde bulunur. (2.41) eşitliğinde toplam sembolü altındaki terimler açılırsa bu fark

$$D_{2k}(x) - D_{2k-2}(x) = (-1)^k \frac{2k}{2k-k} \binom{2k-k}{k} x^{2k-2k} \tag{2.42}$$

$$+[x^{2k} - \frac{2k}{2k-1} \binom{2k-1}{1} x^{2k-2} + \cdots + \frac{2k}{k+1} \binom{k+1}{k-1} x^2$$

$$-(x^{2k-2}+\cdots+(-1)^{k-2}\tfrac{2k-2}{k}\binom{k}{k-2}x^2+(-1)^{k-1}2)]$$

eşitliğine dönüşür. (2.42)'de gerekli hesaplamalar ve düzenlemeler yapılması sonucunda minimal polinomun paydası için istenilen fark

$$D_{2k}(x)-D_{2k-2}(x)=(-1)^k 2-(-1)^{k-1}2+\sum Bx \tag{2.43}$$

olarak bulunur. (2.43)'te son bir düzenleme ile bu fark

$$D_{2k}(x)-D_{2k-2}(x)=(-1)^k 4+\sum Bx \tag{2.44}$$

eşitliğine dönüşür. Böylece (2.44)'te $p=2k-1$ olduğu dikkate alındığında minimal polinomun paydası için istenilen

$$D_{p+1}(x)-D_{p-1}(x)=(-1)^{\frac{p+1}{2}}4+\sum Bx$$

eşitliğe ulaşılmış olur.

Yardımcı Teorem 2.7.2.a, 2.7.2.b, 2.7.2.c ve 2.7.2.d' nin verilmesinden sonra şimdi de ana teoremin yani Teorem 2.7.2'nin ispatına geçiyoruz.

İspat. $q\geq 3$ ve $p>2$ asal olsun.

$x=0$ için $$P_{2p}^*(x)\equiv 0 \ \ mod\, p$$

olduğu gösterilmelidir. $q=2p$ çift ise Teorem 3.6.2 gereğince P_{2p}^* minimal polinomu da çifttir. Buna göre Yardımcı Teorem 2.7.2.a'ya göre

$q=2p$ için $$P_{2p}^*(x)=2^{-1}.\frac{D_{2p+1}(x)+D_{2p-1}(x)}{\prod_{\substack{d|4p\\ d\neq 4p\\ d\nmid 2p}}\psi_d\left(\frac{x}{2}\right).[D_{p+1}(x)-D_{p-1}(x)]} \tag{2.45}$$

minimal polinomu geçerlidir. 2.7.2.b, 2.7.2.c ve 2.7.2.d Yardımcı Teoremlerinin (2.45) eşitliğinde kullanılması ile

$$P_{2p}^*(x)=2^{-1}.\frac{x[-4p+\sum Ax]}{2^{-1}x\left[(-1)^{\frac{p+1}{2}}.4+\sum Bx\right]} \tag{2.46}$$

eşitliği alınır. (2.46) eşitliğinde gerekli sadeleştirmelerin yapılması ile

$$P_{2p}^{*}(x) = \frac{-4p+\sum Ax}{(-1)^{\frac{p+1}{2}}.4+\sum Bx}$$

eşitliği elde edilir. Son olarak minimal polinomda

$x = 0$ için $$P_{2p}^{*}(0) = \frac{-4p+\sum A.0}{(-1)^{\frac{p+1}{2}}.4+\sum B.0}$$

$$P_{2p}^{*}(0) = \frac{-p}{(-1)^{\frac{p+1}{2}}} \tag{2.47}$$

eşitliği elde edilir. (2.47)'de minimal polinomun paydası sıfırdan farklı olduğundan asal moda geçildiğinde istenilen

$$P_{2p}^{*}(0) \equiv 0 \quad mod\, p$$

denkliği elde edilir. O halde P_{2p}^{*} minimal polinomu $mod\, p$'de $x = 0$ köküne sahiptir.

Teorem 2.7.2'den farklı olarak asal kuvvetlerin iki katı biçiminde olan bir minimal polinomun asal modda sıfır köküne sahip olduğunu aşağıdaki sonuç ile veriyoruz.

Teorem 2.7.3. (Ozgur ve ark. 2011c) $q \geq 3$, $p > 2$ asal, $t > 1$, $t \in \mathbb{Z}$ olmak üzere $q = 2p^t$ ise $P_{2p^t}^{*}(x), mod\, p$'ye göre $x = 0$ köküne sahiptir.

Bir önceki sonuçların ispatlarına benzer olarak yine bu sonucun ispatı yapılmadan önce de bu sonucun ispatını kolaylaştıracak bir takım yardımcı teoremler ispatları ile birlikte verilecektir. Öncelikle $q = 2p^t$ durumundaki minimal polinom bulunmalıdır.

Aşağıdaki yardımcı teoremde q sayısının asal kuvvetlerin iki katı olması durumundaki bir minimal polinomun genel biçiminin ne olduğunu veriyoruz.

Yardımcı Teorem 2.7.3.a. $q \geq 3$, $p > 2$ asal, $t > 1$, $t \in \mathbb{Z}$ olmak üzere $q = 2p^t$ iken $P_{2p^t}^{*}$ minimal polinomu,

$$P_{2p^t}^{*}(x) = 2^{-p^{t-1}} . \frac{D_{2p^t+1}(x) - D_{2p^t-1}(x)}{\prod_{k=0}^{t-1} \psi_{4p^k}\left(\frac{x}{2}\right)\left[D_{p^t+1}(x) - D_{p^t+1}(x)\right]}$$

biçimindedir.

İspat. $q \geq 3$, $p > 2$ asal, $t > 1, t \in \mathbb{Z}$ olsun.

$q=2p^t$ çift iken 2.6.2 Teoremi gereğince $P^*_{2p^t}$ minimal polinomu da çifttir. Buna göre

$$q=2p^t \quad \text{için} \quad P^*_{2p^t}(x)=2^{\frac{\varphi(2.2p^t)-2p^t}{2}}.\frac{D_{2p^t+1}(x)-D_{2p^t-1}(x)}{\prod_{\substack{d|2.2p^t\\ d\neq 2.2p^t\\ d\nmid 2p^t}}\psi_d\left(\frac{x}{2}\right).\left[D_{\frac{2p^t}{2}+1}(x)-D_{\frac{2p^t}{2}-1}(x)\right]}$$

$$P^*_{2p^t}(x)=2^{\frac{\varphi(4p^t)-2p^t}{2}}.\frac{D_{2p^t+1}(x)-D_{2p^t-1}(x)}{\prod_{\substack{d|4p^t\\ d\neq 4p^t\\ d\nmid 2p^t}}\psi_d\left(\frac{x}{2}\right).\left[D_{p^t+1}(x)-D_{p^t-1}(x)\right]} \tag{2.48}$$

eşitliği bulunur. (2.48) eşitliğinde φ Euler fonksiyonu olmak üzere

$$\varphi(4p^t)=\varphi(4).\varphi(p^t)=2.(p^t-p^{t-1})=2p^t-2p^{t-1}$$

bağıntısı ele alınır ve gerekli düzenlemeler yapılırsa

$$P^*_{2p^t}(x)=2^{-p^{t-1}}.\frac{D_{2p^t+1}(x)-D_{2p^t-1}(x)}{\prod_{\substack{d|4p^t\\ d\neq 4p^t\\ d\nmid 2p^t}}\psi_d\left(\frac{x}{2}\right)\left[D_{p^t+1}(x)-D_{p^t-1}(x)\right]} \tag{2.49}$$

eşitliği alınır. Son olarak (2.49) eşitliğinde çarpım sembolü altındaki koşullar değerlendirilmelidir. Buna göre $d|4p^t$ iken d bölenleri: $1, 2,\ 4,\ p, 2p, 4p, \dots 2p^{t-1}, 4p^{t-1}$, $2p^t$, $4p^t$'dir. $d\neq 4p^t$ ve $d\nmid 2p^t$ koşulları dikkate alınırsa d bölenleri: $4, 4p, \dots, 4p^{t-1}$ olarak bulunur. Bu bölenler için (2.49) eşitliğindeki çarpım sembolü

$$\prod_{\substack{d|4p^t\\ d\neq 4p^t\\ d\nmid 2p^t}}\psi_d\left(\frac{x}{2}\right)=\psi_4\left(\frac{x}{2}\right).\psi_{4p}\left(\frac{x}{2}\right)\dots\psi_{4p^{t-1}}\left(\frac{x}{2}\right)=\prod_{k=0}^{t-1}\psi_{4p^k}\left(\frac{x}{2}\right) \tag{2.50}$$

eşitliğine dönüşür. (2.50) eşitliğinin (2.49)'daki eşitlikte göz önünde bulundurulması ile istenen minimal polinom,

$$P^*_{2p^t}(x)=2^{-p^{t-1}}.\frac{D_{2p^t+1}(x)-D_{2p^t-1}(x)}{\prod_{k=0}^{t-1}\psi_{4p^k}\left(\frac{x}{2}\right).\left[D_{p^t+1}(x)-D_{p^t-1}(x)\right]}$$

biçiminde bulunur.

$P^*_{2p^t}$ minimal polinomun payına ilişkin bilgiyi aşağıdaki yardımcı teorem ile veriyoruz.

Yardımcı Teorem 2.7.3.b. $p > 2$ asal, $t > 1,\ t \in \mathbb{Z}$ ve A bir sabit olsun. O zaman $P^*_{2p^t}$ minimal polinomun payı

$$D_{2p^t+1}(x) - D_{2p^t-1}(x) = x[-4p^t + \sum Ax]$$

biçimindedir, burada $\sum Ax = x^{2p^t} - (2p^t + 2)x^{2p^t-2} + \cdots$'dir.

İspat. $p > 2$ asal, $t > 1,\ t \in \mathbb{Z}$ olsun. (2.2)'deki Dickson polinomlarının tanımından

$$D_{2p^t+1}(x) = \sum_{i=0}^{\left[\frac{2p^t+1}{2}\right]} (-1)^i \frac{2p^t+1}{2p^t+1-i} \binom{2p^t+1-i}{i} x^{2p^t+1-2i} \tag{2.51}$$

ve

$$D_{2p^t-1}(x) = \sum_{i=0}^{\left[\frac{2p^t-1}{2}\right]} (-1)^i \frac{2p^t-1}{2p^t-1-i} \binom{2p^t-1-i}{i} x^{2p^t-1-2i} \tag{2.52}$$

eşitlikleri alınır. (2.51) ve (2.52)'de toplam sembollerinin üst indisleri düzenlendiğinde

$$D_{2p^t+1}(x) = \sum_{i=0}^{p^t} (-1)^i \frac{2p^t+1}{2p^t+1-i} \binom{2p^t+1-i}{i} x^{2p^t+1-2i} \tag{2.53}$$

ve

$$D_{2p^t-1}(x) = \sum_{i=0}^{p^t-1} (-1)^i \frac{2p^t-1}{2p^t-1-i} \binom{2p^t-1-i}{i} x^{2p^t-1-2i} \tag{2.54}$$

eşitlikleri elde edilir. Buna göre (2.53) ve (2.54)'ten minimal polinomun payı için istenilen $D_{2p^t+1}(x) - D_{2p^t-1}(x)$ farkı

$$D_{2p^t+1}(x) - D_{2p^t-1}(x) = (-1)^{p^t} \frac{2p^t+1}{2p^t+1-p^t} \binom{2p^t+1-p^t}{p^t} x^{2p^t+1-2p^t} \tag{2.55}$$

$$+(-1)^{p^t-1} \frac{2p^t+1}{2p^t+1-p^t+1} \binom{2p^t+1-p^t+1}{p^t-1} x^{2p^t+1-2p^t+2} + \cdots$$

$$+(-1)^1 \frac{2p^t+1}{2p^t} \binom{2p^t+1-1}{1} x^{2p^t-1} + (-1)^0 \frac{2p^t+1}{2p^t+1} \binom{2p^t+1}{0} x^{2p^t+1}$$

$$-\Bigg[(-1)^{p^t-1} \frac{2p^t-1}{2p^t-1-p^t+1} \binom{2p^t-1-p^t+1}{p^t-1} x^{2p^t-1-2p^t+2}$$

$$+(-1)^{p^t-2}\frac{2p^t-1}{2p^t-1-p^t+2}\binom{2p^t-1-p^t+2}{p^t-2}x^{2p^t-1-2p^t+4}+\cdots$$

$$+(-1)^1\frac{2p^t-1}{2p^t-1-1}\binom{2p^t-1-1}{1}x^{2p^t-1-2}+(-1)^0\frac{2p^t-1}{2p^t-1}\binom{2p^t-1}{0}x^{2p^t-1}\Bigg]$$

biçiminde bulunur. (2.55) eşitliğindeki bu fark düzenlenirse

$$D_{2p^t+1}(x)-D_{2p^t-1}(x)=(-1)^{p^t}\frac{2p^t+1}{p^t+1}\binom{p^t+1}{p^t}x \tag{2.56}$$

$$+(-1)^{p^t-1}\frac{2p^t+1}{p^t+2}\binom{p^t+2}{p^t-1}x^3+\cdots+(-1)^1\frac{2p^t+1}{2p^t}\binom{2p^t}{1}x^{2p^t-1}+x^{2p^t+1}$$

$$-\Bigg[(-1)^{p^t-1}\frac{2p^t-1}{p^t}\binom{p^t}{p^t-1}x+(-1)^{p^t-2}\frac{2p^t-1}{p^t+1}\binom{p^t+1}{p^t-2}x^3+\cdots$$

$$+(-1)^1\frac{2p^t-1}{2p^t-2}\binom{2p^t-2}{1}x^{2p^t-3}+x^{2p^t-1}\Bigg]$$

eşitliği bulunur. Son olarak (2.56) eşitliğinde aynı dereceli terimler bir araya getirilip düzenlendiğinde böylece $P^*_{2p^t}$ minimal polinomun payı için istenilen

$$D_{2p^t+1}(x)-D_{2p^t-1}(x)=x^{2p^t+1}+(-2p^t-1-1)x^{2p^t-1}+$$

$$\ldots+(-2p^t-1-2p^t+1)x$$

$$D_{2p^t+1}(x)-D_{2p^t-1}(x)=x^{2p^t+1}-(2p^t+2)x^{2p^t-1}+\cdots+(-4p^t)x \tag{2.57}$$

eşitliği elde edilmiş olunur. (2.57) eşitliği x parentezine alınıp gerekli düzenleme yapıldığında minimal polinomun payı en son istenen

$$D_{2p^t+1}(x)-D_{2p^t-1}(x)=x(x^{2p^t}-(2p^t+2)x^{2p^t-2}+\cdots+(-4p^t))$$

$$D_{2p^t+1}(x)-D_{2p^t-1}(x)=x[-4p^t+\sum Ax]$$

şeklini almış olur.

$P^*_{2p^t}$ minimal polinomun payı elde edildikten sonra aynı minimal polinomun paydası hakkındaki bilgiyi de aşağıdaki yardımcı teoremde veriyoruz.

Yardımcı Teorem 2.7.3.c. $p > 2$ asal, $t > 1$, $t \in \mathbb{Z}$ ve B bir sabit olsun. O zaman $P^*_{2p^t}$ minimal polinomun paydası

$$D_{p^t+1}(x) - D_{p^t-1}(x) = 4.(-1)^{\frac{p^t+1}{2}} + \sum Bx$$

biçimindedir, burada $\sum Bx = x^{p^t+1} - (p^t+2)x^{p^t-1} + \cdots$'dir.

İspat. $p > 2$ asal, $t > 1$, $t \in \mathbb{Z}$ olsun. $P^*_{2p^t}$ minimal polinomun payı kısmındakine benzer olarak (2.2)'deki Dickson polinomlarının tanımından

$$D_{p^t+1}(x) = \sum_{i=0}^{\left[\frac{p^t+1}{2}\right]}(-1)^i \frac{p^t+1}{p^t+1-i}\binom{p^t+1-i}{i} x^{p^t+1-2i} \tag{2.58}$$

ve

$$D_{p^t-1}(x) = \sum_{i=0}^{\left[\frac{p^t-1}{2}\right]}(-1)^i \frac{p^t-1}{p^t-1-i}\binom{p^t-1-i}{i} x^{p^t-1-2i} \tag{2.59}$$

eşitlikleri alınır. (2.58) ve (2.59)'da toplam sembollerinin üst indisleri arasında $\frac{p^t+1}{2} = k,\ k \in \mathbb{Z}$ olmak üzere $p^t = 2k-1$ için

$$\left[\frac{p^t+1}{2}\right] = 1 + \left[\frac{p^t-1}{2}\right] \tag{2.60}$$

bağıntısının olduğu kolaylıkla görülebilir. (2.60) bağıntısı (2.59) ve (2.58) eşitliklerinde yerine konulursa bu eşitliklerin sırasıyla

$$D_{2k}(x) = \sum_{i=0}^{k}(-1)^i \frac{2k}{2k-i}\binom{2k-i}{i} x^{2k-2i} \tag{2.61}$$

ve

$$D_{2k-2}(x) = \sum_{i=0}^{k-1}(-1)^i \frac{2k-2}{2k-2-i}\binom{2k-2-i}{i} x^{2k-2-2i} \tag{2.62}$$

eşitliklerine dönüştüğü görülür. (2.61) ve (2.62)'den minimal polinomun paydası için istenilen $D_{p^t+1}(x) - D_{p^t-1}(x)$ farkı

$$D_{2k}(x) - D_{2k-2}(x) = (-1)^k \frac{2k}{2k-k}\binom{2k-k}{k} x^{2k-2k} + \tag{2.63}$$

$$+(-1)^{k-1}\tfrac{2k}{2k-k+1}\binom{2k-k+1}{k-1}x^{2k-2k+2}+\cdots$$

$$+(-1)^{1}\tfrac{2k}{2k-1}\binom{2k-1}{1}x^{2k-2}+(-1)^{0}\tfrac{2k}{2k}\binom{2k}{0}x^{2k}$$

$$-\Big[(-1)^{k-1}\tfrac{2k-2}{2k-2-k+1}\binom{2k-2-k+1}{k-1}x^{2k-2-2k+2}+\cdots$$

$$+(-1)^{1}\tfrac{2k-2}{2k-3}\binom{2k-3}{1}x^{2k-4}+(-1)^{0}\tfrac{2k-2}{2k-2}\binom{2k}{0}x^{2k-2}\Big]$$

biçiminde bulunur. (2.63) eşitliğindeki fark üzerinde gerekli hesaplamalar yapıldığında

$$D_{2k}(x)-D_{2k-2}(x)=(-1)^{k}\tfrac{2k}{k}\binom{k}{k}+(-1)^{k-1}\tfrac{2k}{k+1}\binom{k+1}{k-1}x^{2}+\cdots$$

$$+(-1)^{1}\tfrac{2k}{2k-1}\binom{2k-1}{1}x^{2k-2}+x^{2k}-\Big[(-1)^{k-1}2\binom{k-1}{k-1}+\cdots$$

$$+(-1)^{1}(2k-2)x^{2k-4}+x^{2k-2}\Big]$$

$$D_{2k}(x)-D_{2k-2}(x)=x^{2k}+(-2k)x^{2k-2}+\cdots+(-1)^{k}.2 \qquad (2.64)$$

$$-[x^{2k-2}+\cdots+(-1)^{k-1}2]$$

eşitliği alınır. (2.64)'te dereceleri aynı olan terimler bir araya getirildiğinde

$$D_{2k}(x)-D_{2k-2}(x)=x^{2k}-(2k+1)x^{2k-2}+\cdots+(-1)^{k}.4$$

eşitliği elde edilir. Böylece $p^t=2k-1$ için $D_{2k}(x)-D_{2k-2}(x)$ farkı minimal polinomun paydası için istenilen

$$D_{p^t+1}(x)-D_{p^t-1}(x)=x^{p^t+1}-(p^t+2)x^{p^t-1}+\cdots+(-1)^{\frac{p^t+1}{2}}.4 \qquad (2.65)$$

biçime dönüşmüş olur. Son olarak (2.65) eşitliğinde gerekli düzenleme yapıldığında minimal polinomun paydası istenilen eşitlik en son

$$D_{p^t+1}(x)-D_{p^t-1}(x)=(-1)^{\frac{p^t+1}{2}}.4+\sum Bx$$

şeklini alır.

Yardımcı Teorem 2.7.3.a, 2.7.3.b, 2.7.3.c ve ispatlarının verilmesinden sonra Teorem 2.7.3'ün ispatına geçiyoruz.

İspat. $q \geq 3$ bileşik, $p > 2$ asal, $t > 1,\ t \in \mathbb{Z}$ olsun.

$x = 0$ için $P^*_{2p^t}(x) \equiv 0 \ mod\, p$ olduğu gösterilmelidir.

$q = 2p^t$ çift iken Teorem 2.6.2 gereğince $P^*_{2p^t}$ minimal polinomu da çifttir. Buna göre $q = 2p^t$ için Yardımcı Teorem 2.7.3.a'dan minimal polinom

$$P^*_{2p^t}(x) = 2^{-p^{t-1}}.\frac{D_{2p^t+1}(x)-D_{2p^t-1}(x)}{\prod_{k=0}^{t-1}\psi_{4p^k}\left(\frac{x}{2}\right)\left[D_{p^t+1}(x)-D_{p^t+1}(x)\right]} \tag{2.66}$$

biçimindedir. (2.66)'daki minimal polinomun payı için Yardımcı Teorem 2.7.3.b ve paydası için de Yardımcı Teorem 2.7.3.c uygulandığında

$$P^*_{2p^t}(x) = 2^{-p^{t-1}}.\frac{x[-4p^t+\sum Ax]}{\psi_4\left(\frac{x}{2}\right).\psi_{4p}\left(\frac{x}{2}\right)...\psi_{4p^{t-1}}\left(\frac{x}{2}\right)[(-1)^{\frac{p^t+1}{2}}.4+\sum Bx]} \tag{2.67}$$

eşitliği alınır. (2.67)'deki minimal polinomun pay kısmı x parantezine alınır ve payda kısmında da $\psi_4\left(\frac{x}{2}\right) = \frac{x}{2}$ olduğu dikkate alınırsa

$$P^*_{2p^t}(x) = 2^{-p^{t-1}}.\frac{x[-4p^t+\sum Ax]}{\frac{x}{2}.\psi_{4p}\left(\frac{x}{2}\right)...\psi_{4p^{t-1}}\left(\frac{x}{2}\right)[(-1)^{\frac{p^t+1}{2}}.4+\sum Bx]} \tag{2.68}$$

eşitliği elde edilir. (2.68)'de gerekli sadeleştirmelerin yapılmasıyla minimal polinom istenilen en son

$$P^*_{2p^t}(x) = 2^{-p^{t-1}}.\frac{-4p^t+\sum Ax}{\frac{1}{2}\left(-cos\frac{\pi}{2p}\right)...\left(-cos\frac{\pi}{2p^{t-1}}\right)[(-1)^{\frac{p^t+1}{2}}.4+\sum Bx]} \tag{2.69}$$

şeklini alır. Son olarak (2.69) eşitliğindeki minimal polinom

$$x = 0 \text{ için} \quad P^*_{2p^t}(0) = 2^{-p^{t-1}}.\frac{-4p^t}{\frac{1}{2}\left(-cos\frac{\pi}{2p}\right)...\left(-cos\frac{\pi}{2p^{t-1}}\right)(-1)^{\frac{p^t+1}{2}}.4} \tag{2.70}$$

eşitliğine dönüşür. (2.70)'teki minimal polinomun paydası dikkat edilirse $p > 2$ asal ve $t > 1\,,\ t \in \mathbb{Z}$ için sıfırdan farklıdır. Böylece (2.70) eşitliğinde asal moda geçildiğinde

$$P^*_{2p^t}(0) \equiv 0 \qquad mod\ p$$

denkliği elde edilir. O halde $x = 0$, $P^*_{2p^t}$ minimal polinomunun asal modda bir köküdür.

Aşağıda hesaplama yoluyla tahmin edilen bazı sonuçları listeliyoruz. Bunlara benzer bir çok sonuç elde edilebilir. Ancak matematiksel ispatları için yeni bir yönteme ihtiyaç duyulmaktadır:

İddia 2.8. $p > 2$ asal olmak üzere $q = p$ ise $P^*_p(p-2) \equiv 0\ mod\ p$'dir.

İddia 2.9. $p > 2$ asal ve $k > 1$ olmak üzere $q = p^k$ ise

$$P^*_{p^k}(p-2) \equiv 0\ mod\ p$$

denkliği geçerlidir, $q = 3^k$ olması halinde ise $P^*_{3^k}(1) \equiv 0\ mod\ 3$'dir.

İddia 2.10. $p > 3$ olmak üzere $q = 3p$ ise $P^*_{3p}(1) \equiv 0\ mod\ p$'dir.

İddia 2.11. $t \geq 1$ olmak üzere $q = 3.2^t$ ise $P^*_{3.2^t}(1) \equiv 0\ mod\ 2$'dir.

3. ψ_{2q} ve P_q^* MİNİMAL POLİNOMLARININ MAPLE İLE HESAPLANIŞI

3.1. Giriş

Bir önceki bölümde $q \geq 3$, $q \in \mathbb{Z}$ olmak üzere $x = \cos(\pi/q)$'nun minimal polinomu ψ_{2q} ve $x = 2cos\,\pi/q$'nun minimal polinomu P_q^* ile temsil edilmişti. Ayrıca Watkins ve Zeitlin'in (1993) çalışmasında $n = 2q$ olmak üzere ψ_{2q}'nun ve bu minimal polinoma bağlı olarak Cangül'ün (1993) çalışmasında da λ_q'nun hesaplanmasına ilişkin formüller verilmiştir. Ancak Cangül'ün (1993) çalışmasında $1 \leq n \leq 13$ için ψ_n ve $1 \leq q \leq 50$ için λ_q minimal polinomlarının bir tablosu verilmiştir. Bu çalışmanın bu bölümünde Cangül (1993)'ün çalışmasına ek olarak MAPLE ile $n > 13$ için ψ_n ve $q > 50$ için λ_q minimal polinomlarının genişleyen bir listesi elde edilmiştir. Böylece bu liste bundan sonra yapılmak istenen pek çok çalışmaya ışık olacaktır. Öncelikle ψ_{2q} minimal polinomlarının MAPLE'da nasıl hesaplandığı anlatılmıştır.

3.2. ψ_{2q} Minimal Polinomlarının Maple ile Hesaplanması

$n \in \mathbb{N}$ olmak üzere $x = \cos(2\pi/n)$'nin ψ_n minimal polinomunun MAPLE ile hesabı, Watkins ve Zeitlin (1993)'nin çalışması temel alınarak yapılmıştır. Buna göre belli özellikteki $n \in \mathbb{N}$ sayıları için belli bir gruplar oluşturulmuştur. Daha sonra her bir grup için ψ_n minimal polinomunun hesabına yönelik kurallar geliştirilmiştir. En sonunda da bu kuralların, bir döngü içinde MAPLE'da algoritması yazılıp Maple tarafından ψ_n minimal polinomlarınınn hesabının yapılması istenmiştir. Daha önce kuralı verilerek Maple'a anlatılan minimal polinomlar, böylece MAPLE tarafından hızlı bir şekilde hesaplanarak liste halinde verilir.

$n \in \mathbb{N}$ sayılarının içinde belli bir özelliğe uymayan sayıların olduğu da unutulmamalıdır. Bu durumda bu özellikteki sayıların ψ_n minimal polinomlarının hesabı için kural geliştirilemiyeceğinden döngü ile bu polinomların hesabı Maple'a ifade edilemez. Bu sebeple ψ_n minimal polinomlarının hesabı için Watkins ve Zeitlin (1993)'nin çalışmasına başvurulmuştur. Buna göre $n \in \mathbb{N}$'nin tek ve çift olduğu durumlar için ψ_n minimal polinomlarının hesabı, Chebycheff polinomlarından da yararlanılarak Maple'da algoritması yazılıp istenen $n \in \mathbb{N}$ değeri için ψ_n, Maple tarafından kolaylıkla hesaplanır. Böylece $n \in \mathbb{N}$ için el ile hesaplanması oldukça güç olan birçok ψ_n minimal polinomları Maple ile kolaylıkla ve hızlı bir şekilde hesap edilir.

Aşağıda belli özellikteki $n \in \mathbb{N}$ sayıları için MAPLE ile ψ_n'lerin hesabı anlatılmaktadır. Bu çalışma Ozgur ve ark (2012c) tarafından yapılmıştır.

3.2.1. $n = p$ için ψ_p minimal polinomları:

$n \in \mathbb{N}$, $n = p > 2$ asal olsun. Teorem 2.4.1. gereği $n = p$ tek olmak üzere $x = \cos(2\pi/p)$'nin ψ_p minimal polinomunun hesabı için (2.3) eşitliği kullanılırsa

$n = 2.1 + 1 = 3$ için
$$T_2(x) - T_1(x) = 2^1 \prod_{d|3} \psi_d(x) \tag{3.1}$$
$$= 2\psi_1(x)\psi_3(x)$$

şeklinde olur. (3.1) eşitliğinde $n = 1$ için $x = \cos(2\pi/1) = 1$ olmak üzere $\psi_1(x) = x - 1$'dir. Böylece (3.1)'de istenilen $\psi_3(x)$ yalnız bırakılırsa

$n = 3$ için
$$\frac{T_2(x) - T_1(x)}{2(x-1)} = \psi_3(x)$$

eşitliği alınır. Benzer şekilde

$n = 2.2 + 1 = 5$ için
$$T_3(x) - T_2(x) = 2^2 \prod_{d|5} \psi_d(x) \tag{3.2}$$
$$= 2^2\psi_1(x)\psi_5(x)$$

eşitliği elde edilir. (3.2) eşitliğinde yine (3.1)'dekine benzer olarak $\psi_1(x) = x - 1$'dir ve $\psi_5(x)$ yalnız bırakılırsa

$n = 5$ için
$$\frac{T_3(x) - T_2(x)}{2^2(x-1)} = \psi_5(x)$$

eşitliği bulunur. Benzer işlemler diğer asallar için yapılırsa

$n = 7$ için
$$\frac{T_4(x) - T_3(x)}{2^3(x-1)} = \psi_7(x)$$

$n = 11$ için $\frac{T_6(x)-T_5(x)}{2^5(x-1)} = \psi_{11}(x)$

$\vdots$ $\vdots$

belli bir kuralı izleyen eşitlikler ortaya çıkar. Buna göre bu eşitliklerdeki kuralı aşağıdaki teoremde veriyoruz.

Teorem 3.2.1.1. $p > 2$ asal sayı ve $n = p$ olsun. O zaman $p = 2s + 1$ $(s \in \mathbb{N})$ olmak üzere $\psi_p(x)$ minimal polinomu,

$$\psi_p(x) = \psi_{2s+1}(x) = \frac{T_{s+1}(x)-T_s(x)}{2^s(x-1)} \tag{3.3}$$

biçimindedir.

İspat. $n = p > 2$ asal sayı ve $p = 2s + 1$ $(s \in \mathbb{N})$ olsun. Teorem 2.4.1. gereği $x = \cos(2\pi/p)$'nin ψ_p minimal polinomunun hesabı için (2.3) eşitliği kullanılırsa

$n = p = 2s + 1$ için
$$\begin{aligned} T_{s+1}(x) - T_s(x) &= 2^s \prod_{d|p} \psi_d(x) \\ &= 2^s \psi_1(x)\psi_p(x) \end{aligned} \tag{3.4}$$

eşitliği alınır. (3.4)'te $\psi_1(x) = x - 1$ olmak üzere $\psi_p(x)$ yalnız bırakılırsa istenilen eşitlik

$n = p = 2s + 1$ için $\psi_p(x) = \psi_{2s+1}(x) \frac{T_{s+1}(x)-T_s(x)}{2^s(x-1)}$

şeklinde bulunur.

Aşağıda $n = p$ tek asal olmak üzere ψ_p minimal polinomunun hesabı için yaptığımız programlama Teorem 3.2.2.1.'in uygulaması niteliğindedir.

$n = p$ tek asal olmak üzere ψ_p minimal polinomunun hesabı için (3.3) kuralı Maple'da bir döngü içinde ifade edilmelidir. (3.3)'e dikkat edildiğinde içinde Chebycheff polinomlarının olduğu görülür. Maple'da döngüyü ifade etmeden önce bu Chebycehff polinomları, " [*G*, *H*, *L*, *P*, *T*, *U*] " adlı paketin içinden çağrılmalıdır.

Böylece Maple, bu paketin çağrılması ile istenen Chebycheff polinomlarının hesabını yapmaktadır. “ $[G, H, L, P, T, U]$ ” adlı paketin çağrılmasından sonra artık Maple , (3.3) kuralına ait döngünün hesabı için hazırdır.

Aşağıda Maple’da (3.3)’e ait algoritma ve bu algoritmaya ait çıktı görülmektedir. Bu algoritma içindeki döngü ile s’nin daha büyük değerleri de hesaplanabilineceğinden s değerleri $1 \leq s \leq 26$ için sınırlandırılmıştır.

```
> with(orthopoly);
```

$$[G, H, L, P, T, U]$$

```
> f:=proc(x)local s,A,B,C;with(orthopoly);for s from 1 to 26 do if isprime (2*s+1) then A:=sort(T(s+1,x)-T(s,x));evala(Divide(A,x1,'q'));q;C:=sort((1/2)^s*q);print(2*s+1,sort(C));end if;end do;end proc;
```

```
f := proc(x)
local s, A, B, C;
    with(orthopoly);
    for s to 26 do
        if isprime(2×s + 1) then
            A := sort(T(s + 1, x) − T(s, x));
            evala(Divide(A, x1, 'q'));
            q;
            C := sort((1/2)^s×q);
            print(2×s + 1, sort(C))
        end if
    end do
end proc
```

```
> f(x);
```

$$3, x+\frac{1}{2}$$

$$5, x^2+\frac{1}{2}x-\frac{1}{4}$$

$$7, x^3+\frac{1}{2}x^2-\frac{1}{2}x-\frac{1}{8}$$

$$11, x^5+\frac{1}{2}x^4-x^3-\frac{3}{8}x^2+\frac{3}{16}x+\frac{1}{32}$$

$$13, x^6+\frac{1}{2}x^5-\frac{5}{4}x^4-\frac{1}{2}x^3+\frac{3}{8}x^2+\frac{3}{32}x-\frac{1}{64}$$

$$17, x^8+\frac{1}{2}x^7-\frac{7}{4}x^6-\frac{3}{4}x^5+\frac{15}{16}x^4+\frac{5}{16}x^3-\frac{5}{32}x^2-\frac{1}{32}x+\frac{1}{256}$$

$$19, x^9+\frac{1}{2}x^8-2x^7-\frac{7}{8}x^6+\frac{21}{16}x^5+\frac{15}{32}x^4-\frac{5}{16}x^3-\frac{5}{64}x^2+\frac{5}{256}x+\frac{1}{512}$$

$$23, x^{11}+\frac{1}{2}x^{10}-\frac{5}{2}x^9-\frac{9}{8}x^8+\frac{9}{4}x^7+\frac{7}{8}x^6-\frac{7}{8}x^5-\frac{35}{128}x^4+\frac{35}{256}x^3+\frac{15}{512}x^2-\frac{3}{512}x-\frac{1}{2048}$$

$$29, x^{14}+\frac{1}{2}x^{13}-\frac{13}{4}x^{12}-\frac{3}{2}x^{11}+\frac{33}{8}x^{10}+\frac{55}{32}x^9-\frac{165}{64}x^8-\frac{15}{16}x^7+\frac{105}{128}x^6+\frac{63}{256}x^5$$
$$-\frac{63}{512}x^4-\frac{7}{256}x^3+\frac{7}{1024}x^2+\frac{7}{8192}x-\frac{1}{16384}$$

$$31, x^{15}+\frac{1}{2}x^{14}-\frac{7}{2}x^{13}-\frac{13}{8}x^{12}+\frac{39}{8}x^{11}+\frac{33}{16}x^{10}-\frac{55}{16}x^9-\frac{165}{128}x^8+\frac{165}{128}x^7+\frac{105}{256}x^6$$
$$-\frac{63}{256}x^5-\frac{63}{1024}x^4+\frac{21}{1024}x^3+\frac{7}{2048}x^2-\frac{1}{2048}x-\frac{1}{32768}$$

$$37, x^{18}+\frac{1}{2}x^{17}-\frac{17}{4}x^{16}-2x^{15}+\frac{15}{2}x^{14}+\frac{105}{32}x^{13}-\frac{455}{64}x^{12}-\frac{91}{32}x^{11}+\frac{1001}{256}x^{10}+\frac{715}{512}x^9$$
$$-\frac{1287}{1024}x^8-\frac{99}{256}x^7+\frac{231}{1024}x^6+\frac{231}{4096}x^5-\frac{165}{8192}x^4-\frac{15}{4096}x^3+\frac{45}{65536}x^2+\frac{9}{131072}x$$
$$-\frac{1}{262144}$$

$$41, x^{20}+\frac{1}{2}x^{19}-\frac{19}{4}x^{18}-\frac{9}{4}x^{17}+\frac{153}{16}x^{16}+\frac{17}{4}x^{15}-\frac{85}{8}x^{14}-\frac{35}{8}x^{13}+\frac{455}{64}x^{12}+\frac{1365}{512}x^{11}$$
$$-\frac{3003}{1024}x^{10}-\frac{1001}{1024}x^9+\frac{3003}{4096}x^8+\frac{429}{2048}x^7-\frac{429}{4096}x^6-\frac{99}{4096}x^5+\frac{495}{65536}x^4$$
$$+\frac{165}{131072}x^3-\frac{55}{262144}x^2-\frac{5}{262144}x+\frac{1}{1048576}$$

$$43,\ x^{21}+\frac{1}{2}x^{20}-5\,x^{19}-\frac{19}{8}x^{18}+\frac{171}{16}x^{17}+\frac{153}{32}x^{16}-\frac{51}{4}x^{15}-\frac{85}{16}x^{14}+\frac{595}{64}x^{13}+\frac{455}{128}x^{12}$$
$$-\frac{273}{64}x^{11}-\frac{3003}{2048}x^{10}+\frac{5005}{4096}x^{9}+\frac{3003}{8192}x^{8}-\frac{429}{2048}x^{7}-\frac{429}{8192}x^{6}+\frac{1287}{65536}x^{5}$$
$$+\frac{495}{131072}x^{4}-\frac{55}{65536}x^{3}-\frac{55}{524288}x^{2}+\frac{11}{1048576}x+\frac{1}{2097152}$$

$$47,\ x^{23}+\frac{1}{2}x^{22}-\frac{11}{2}x^{21}-\frac{21}{8}x^{20}+\frac{105}{8}x^{19}+\frac{95}{16}x^{18}-\frac{285}{16}x^{17}-\frac{969}{128}x^{16}+\frac{969}{64}x^{15}+\frac{765}{128}x^{14}$$
$$-\frac{1071}{128}x^{13}-\frac{1547}{512}x^{12}+\frac{1547}{512}x^{11}+\frac{1001}{1024}x^{10}-\frac{715}{1024}x^{9}-\frac{6435}{32768}x^{8}+\frac{6435}{65536}x^{7}$$
$$+\frac{3003}{131072}x^{6}-\frac{1001}{131072}x^{5}-\frac{715}{524288}x^{4}+\frac{143}{524288}x^{3}+\frac{33}{1048576}x^{2}-\frac{3}{1048576}x$$
$$-\frac{1}{8388608}$$

$$53,\ x^{26}+\frac{1}{2}x^{25}-\frac{25}{4}x^{24}-3\,x^{23}+\frac{69}{4}x^{22}+\frac{253}{32}x^{21}-\frac{1771}{64}x^{20}-\frac{385}{32}x^{19}+\frac{7315}{256}x^{18}$$
$$+\frac{5985}{512}x^{17}-\frac{20349}{1024}x^{16}-\frac{969}{128}x^{15}+\frac{4845}{512}x^{14}+\frac{6783}{2048}x^{13}-\frac{12597}{4096}x^{12}-\frac{1989}{2048}x^{11}$$
$$+\frac{21879}{32768}x^{10}+\frac{12155}{65536}x^{9}-\frac{12155}{131072}x^{8}-\frac{715}{32768}x^{7}+\frac{1001}{131072}x^{6}+\frac{3003}{2097152}x^{5}$$
$$-\frac{1365}{4194304}x^{4}-\frac{91}{2097152}x^{3}+\frac{91}{16777216}x^{2}+\frac{13}{33554432}x-\frac{1}{67108864}$$

$$\vdots$$

3.2.2. $n = 2p$ için ψ_{2p} minimal polinomları

$n \in \mathbb{N}$, $p > 2$ asal sayı ve $n = 2p$ olsun. Teorem 2.4.1.'den $n = 2p$ çift olmak üzere $x = \cos(2\pi/2p)$'nin ψ_{2p} minimal polinomunun hesabı için (2.4) eşitliği kullanılırsa

$$n = 2.3 = 6 \text{ için} \qquad T_4(x) - T_2(x) = 2^3 \textstyle\prod_{d|6} \psi_d(x) \tag{3.5}$$
$$= 2^3\psi_1(x)\psi_2(x)\psi_3(x)\psi_6(x)$$

biçiminde olur. (3.5)'te $n = 2$ için $x = cos(2\pi/2) = -1$ olmak üzere $\psi_2(x) = x + 1$'dir. Ayrıca (3.1) eşitliği (3.5)'te kullanıldığında

$$T_4(x) - T_2(x) = 2^3(x+1)\tfrac{1}{2}\big(T_2(x) - T_1(x)\big)\psi_6(x) \tag{3.6}$$

eşitliği alınır. (3.6)'da $\psi_6(x)$ yalnız bırakılırsa istenen son eşitlik

$n = 2.3 = 6$ için $$\frac{T_4(x)-T_2(x)}{2^2(x+1)\big(T_2(x)-T_1(x)\big)} = \psi_6(x) \tag{3.7}$$

şeklinde bulunur. Benzer şekilde

$n = 2.5 = 10$ için $$T_6(x) - T_4(x) = 2^5 \prod_{d|10} \psi_d(x) \tag{3.8}$$

$$= 2^5\psi_1(x)\psi_2(x)\psi_5(x)\psi_{10}(x)$$

eşitliği elde edilir. (3.8)'de $\psi_2(x) = x + 1$ ve (4.1) eşitlikleri göz önünde bulundurulursa

$$T_6(x) - T_4(x) = 2^5(x + 1)\frac{1}{2^2}\big(T_3(x) - T_2(x)\big)\psi_{10}(x) \tag{3.9}$$

eşitliği alınır. (3.9)'da $\psi_{10}(x)$ yalnız bırakılırsa (3.7)'ye benzer olarak aranan son eşitlik

$n = 2.5 = 2(2.2 + 1) = 10$ için $$\frac{T_6(x)-T_4(x)}{2^3(x+1)\big(T_3(x)-T_2(x)\big)} = \psi_{10}(x) \tag{3.10}$$

biçiminde olur. Asalların iki katı için (3.7) ve (3.10)'daki gibi benzer işlemler yapılmaya devam edildiğinde

$n = 2.7 = 2(2.3 + 1) = 14$ için $$\frac{T_8(x)-T_6(x)}{2^4(x+1)\big(T_4(x)-T_3(x)\big)} = \psi_{14}(x)$$

$n = 2.11 = 2(2.5 + 1) = 22$ için $$\frac{T_{12}(x)-T_{10}(x)}{2^6(x+1)\big(T_6(x)-T_5(x)\big)} = \psi_{22}(x)$$

$n = 2.13 = 2(2.6 + 1) = 26$ için $$\frac{T_{14}(x)-T_{12}(x)}{2^7(x+1)\big(T_7(x)-T_6(x)\big)} = \psi_{26}(x)$$

$\vdots$ $\vdots$

şeklinde belli bir kuralı takip eden eşitlikler ortaya çıkar. Buna göre bu eşitliklerdeki kuralı aşağıdaki teorem ile veriyoruz.

Teorem 3.2.2.1. $p > 2$ asal sayı ve $n = 2p$ olsun. O zaman $p = 2s + 1$ $(s \in \mathbb{N})$ olmak üzere $\psi_{2p}(x)$ minimal polinomu,

$$\psi_{2p}(x) = \psi_{2(2s+1)}(x) = \frac{T_{2s+2}(x)-T_{2s}(x)}{2^{s+1}(x+1)\big(T_{s+1}(x)-T_s(x)\big)} \tag{3.11}$$

şeklindedir.

İspat. $p > 2$ asal sayı ve $n = 2p$ olsun. $p = 2s + 1$ $(s \in \mathbb{N})$ için Teorem 2.4.1.'den $n = 2p$ çift olmak üzere $x = \cos(2\pi/2p)$'nin ψ_{2p} minimal polinomunun hesabı için (2.4) eşitliği kullanılırsa

$n = 2p = 2(2s + 1)$ için

$$T_{2s+1+1}(x) - T_{2s+1-1}(x) = 2^{2s+1} \prod_{d|2p} \psi_d(x) \tag{3.12}$$

$$=2^{2s+1}\psi_1(x)\psi_2(x)\psi_p(x)\psi_{2p}(x)$$

eşitliği elde edilir. (3.12)'de $\psi_2(x) = x + 1$ ve (4.4) eşitliği göz önünde bulundurulursa

$$T_{2s+2}(x) - T_{2s}(x) = 2^{2s+1}(x + 1)\tfrac{1}{2^s}\big(T_{s+1}(x) - T_s(x)\big)\psi_{2p}(x) \tag{3.13}$$

eşitliği alınır. (3.13)'te $\psi_{2p}(x)$ yalnız bırakılırsa istenilen eşitlik

$n = 2(2s + 1)$ için $\qquad \psi_{2p}(x) = \psi_{2(2s+1)}(x) = \frac{T_{2s+2}(x) - T_{2s}(x)}{2^{s+1}(x+1)\big(T_{s+1}(x) - T_s(x)\big)}$

şeklinde elde edilir.

Aşağıda $n = 2p \in \mathbb{N}$ olmak üzere $\psi_{2p}(x)$ minimal polinomun hesabı için yaptığımız algoritma Teorem 3.2.2.1'in uygulamasıdır.

$s \in \mathbb{N}$ olmak üzere $\psi_{2(2s+1)}(x)$ minimal polinomun hesabı için (3.11) kuralı Maple'da bir döngü içinde ifade edilmelidir. 3.2.1'dekine benzer olarak öncelikle Cheybcheff polinomlarının hesabının yapılacağı " $[G, H, L, P, T, U]$ " isimli paket çağrılmalıdır. Daha sonra (3.11) kuralına ilişkin döngü Maple'da s'nin belli aralıklardaki değerleri için ifade edildiğinde Maple artık bu döngüyü hesaplamaya hazır hale gelmiştir.

Aşağıda (3.11) kuralına ilişkin algoritma ve çıktısı Maple ile hesaplanmıştır. Burada yine bu algoritma içindeki döngünün üst sınır değeri istenildği kadar arttırılabileceğinden bu kısımda s'nin aralıkları sınırlandırılmıştır.

```
> with(orthopoly);
```

$$[G, H, L, P, T, U]$$

```
> f:=proc(x)local s,A,B,C,E;with(orthopoly);for s from 1 to 36 do if isprime(2*s+1) then A:=sort(T(2*s+2,x)-T(2*s,x));B:=sort(T(s+1,x)-T(s,x));C:=expand((x+1)*B);evala(Divide(A,C,'q'));E:=((1/2)^(s+1))*q;print(2*(2*s+1),sort(E));end if;end do;end proc;
```

$f :=$ **proc** (x)
local $s, A, B, C, E;$
with(*orthopoly*);
for s **to** 36 **do**
if isprime($2\times s + 1$) **then**
$A :=$ sort(T($2\times s + 2, x$) $-$ T($2\times s, x$));
$B :=$ sort(T($s + 1, x$) $-$ T(s, x));
$C :=$ expand($(x + 1)\times B$);
evala(Divide($A, C, 'q'$));
$E := (1/2)\hat{}(s + 1)\times q$;
print($4\times s + 2$, sort(E))
end if
end do
end proc

```
> f(x);
```

$$6, x-\frac{1}{2}$$

$$10, x^2-\frac{1}{2}x-\frac{1}{4}$$

$$14, x^3-\frac{1}{2}x^2-\frac{1}{2}x+\frac{1}{8}$$

$$22, x^5-\frac{1}{2}x^4-x^3+\frac{3}{8}x^2+\frac{3}{16}x-\frac{1}{32}$$

$$26, x^6-\frac{1}{2}x^5-\frac{5}{4}x^4+\frac{1}{2}x^3+\frac{3}{8}x^2-\frac{3}{32}x-\frac{1}{64}$$

$$34, x^8-\frac{1}{2}x^7-\frac{7}{4}x^6+\frac{3}{4}x^5+\frac{15}{16}x^4-\frac{5}{16}x^3-\frac{5}{32}x^2+\frac{1}{32}x+\frac{1}{256}$$

$$38, x^9-\frac{1}{2}x^8-2x^7+\frac{7}{8}x^6+\frac{21}{16}x^5-\frac{15}{32}x^4-\frac{5}{16}x^3+\frac{5}{64}x^2+\frac{5}{256}x-\frac{1}{512}$$

$$46, x^{11}-\frac{1}{2}x^{10}-\frac{5}{2}x^9+\frac{9}{8}x^8+\frac{9}{4}x^7-\frac{7}{8}x^6-\frac{7}{8}x^5+\frac{35}{128}x^4+\frac{35}{256}x^3-\frac{15}{512}x^2-\frac{3}{512}x+\frac{1}{2048}$$

$$58,\ x^{14}-\frac{1}{2}x^{13}-\frac{13}{4}x^{12}+\frac{3}{2}x^{11}+\frac{33}{8}x^{10}-\frac{55}{32}x^{9}-\frac{165}{64}x^{8}+\frac{15}{16}x^{7}+\frac{105}{128}x^{6}-\frac{63}{256}x^{5}$$
$$-\frac{63}{512}x^{4}+\frac{7}{256}x^{3}+\frac{7}{1024}x^{2}-\frac{7}{8192}x-\frac{1}{16384}$$

$$62,\ x^{15}-\frac{1}{2}x^{14}-\frac{7}{2}x^{13}+\frac{13}{8}x^{12}+\frac{39}{8}x^{11}-\frac{33}{16}x^{10}-\frac{55}{16}x^{9}+\frac{165}{128}x^{8}+\frac{165}{128}x^{7}-\frac{105}{256}x^{6}$$
$$-\frac{63}{256}x^{5}+\frac{63}{1024}x^{4}+\frac{21}{1024}x^{3}-\frac{7}{2048}x^{2}-\frac{1}{2048}x+\frac{1}{32768}$$

$$74,\ x^{18}-\frac{1}{2}x^{17}-\frac{17}{4}x^{16}+2\,x^{15}+\frac{15}{2}x^{14}-\frac{105}{32}x^{13}-\frac{455}{64}x^{12}+\frac{91}{32}x^{11}+\frac{1001}{256}x^{10}-\frac{715}{512}x^{9}$$
$$-\frac{1287}{1024}x^{8}+\frac{99}{256}x^{7}+\frac{231}{1024}x^{6}-\frac{231}{4096}x^{5}-\frac{165}{8192}x^{4}+\frac{15}{4096}x^{3}+\frac{45}{65536}x^{2}-\frac{9}{131072}x$$
$$-\frac{1}{262144}$$

$$82,\ x^{20}-\frac{1}{2}x^{19}-\frac{19}{4}x^{18}+\frac{9}{4}x^{17}+\frac{153}{16}x^{16}-\frac{17}{4}x^{15}-\frac{85}{8}x^{14}+\frac{35}{8}x^{13}+\frac{455}{64}x^{12}-\frac{1365}{512}x^{11}$$
$$-\frac{3003}{1024}x^{10}+\frac{1001}{1024}x^{9}+\frac{3003}{4096}x^{8}-\frac{429}{2048}x^{7}-\frac{429}{4096}x^{6}+\frac{99}{4096}x^{5}+\frac{495}{65536}x^{4}$$
$$-\frac{165}{131072}x^{3}-\frac{55}{262144}x^{2}+\frac{5}{262144}x+\frac{1}{1048576}$$

$$86,\ x^{21}-\frac{1}{2}x^{20}-5\,x^{19}+\frac{19}{8}x^{18}+\frac{171}{16}x^{17}-\frac{153}{32}x^{16}-\frac{51}{4}x^{15}+\frac{85}{16}x^{14}+\frac{595}{64}x^{13}-\frac{455}{128}x^{12}$$
$$-\frac{273}{64}x^{11}+\frac{3003}{2048}x^{10}+\frac{5005}{4096}x^{9}-\frac{3003}{8192}x^{8}-\frac{429}{2048}x^{7}+\frac{429}{8192}x^{6}+\frac{1287}{65536}x^{5}$$
$$-\frac{495}{131072}x^{4}-\frac{55}{65536}x^{3}+\frac{55}{524288}x^{2}+\frac{11}{1048576}x-\frac{1}{2097152}$$

$$\vdots$$

3.2.3. $n = p^2$ için ψ_{p^2} minimal polinomları

$n \in \mathbb{N}$, $p > 2$ asal sayı ve $n = p^2$ olsun. Teorem 2.4.1.'den $n = p^2$ tek için $x = cos(2\pi/p^2)$'nin minimal polinomunun hesabı 3.2.1. ve 3.2.2.'dekilere benzer olarak (2.3) eşitliği kullanıldığında

$$n = 3^2 = (2.1+1)^2 = 9 \text{ için} \qquad T_5(x) - T_4(x) = 2^4 \prod_{d|9} \psi_d(x) \qquad (3.14)$$
$$= 2^4 \psi_1(x)\psi_3(x)\psi_9(x)$$

eşitliği alınır. (3.14)'e (3.1) uygulandığında

$n = 3^2$ için $$T_5(x) - T_4(x) = 2^4 \frac{1}{2}\big(T_2(x) - T_1(x)\big)\psi_9(x) \tag{3.15}$$

eşitliği elde edilir. Son olarak (3.15)'te $\psi_9(x)$ yalnız bırakılırsa istenen eşitlik

$n = 3^2$ için $$\frac{T_5(x)-T_4(x)}{2^3\big(T_2(x)-T_1(x)\big)} = \psi_9(x) \tag{3.16}$$

şeklinde bulunur.

Benzer şekilde

$n = (2.2 + 1)^2 = 25$ için $$T_{13}(x) - T_{12}(x) = 2^{12} \prod_{d|25} \psi_d(x) \tag{3.17}$$

$$= 2^{12}\psi_1(x)\psi_5(x)\psi_{25}(x)$$

eşitliği alınır. (3.17)'de (3.2) kullanılırsa

$n = 5^2$ için $$T_{13}(x) - T_{12}(x) = 2^{12} \frac{1}{2^2}\big(T_3(x) - T_2(x)\big)\psi_{25}(x) \tag{3.18}$$

eşitliği elde edilir. Son olarak (3.18)'de istenen $\psi_{25}(x)$ minimal polinomu

$n = 5^2$ için $$\frac{T_{13}(x)-T_{12}(x)}{2^{10}\big(T_3(x)-T_2(x)\big)} = \psi_{25}(x) \tag{3.19}$$

biçiminde bulunur.

Asalların kareleri için (3.16) ve (3.19)'daki eşitliklere benzer hesaplamalar yapılmaya devam edilirse

$n = (2.3 + 1)^2 = 7^2 = 49$ için $$\frac{T_{25}(x)-T_{24}(x)}{2^{21}\big(T_4(x)-T_3(x)\big)} = \psi_{49}(x)$$

$n = (2.5 + 1)^2 = 11^2 = 121$ için $$\frac{T_{61}(x)-T_{60}(x)}{2^{55}\big(T_5(x)-T_4(x)\big)} = \psi_{121}(x)$$

$n = (2.6 + 1)^2 = 13^2 = 169$ için $$\frac{T_{85}(x)-T_{84}(x)}{2^{78}\big(T_6(x)-T_5(x)\big)} = \psi_{169}(x)$$

$$\vdots \qquad\qquad \vdots$$

biçiminde belli bir kuralı takip eden eşitlikler elde edilir. Buna göre bu kuralı aşağıdaki teoremde veriyoruz.

Teorem 3.2.3.1. $p > 2$ asal sayı ve $n = p^2$ olsun. O zaman $p = 2s + 1$ ($s \in \mathbb{N}$) olmak üzere $\psi_{p^2}(x)$ minimal polinomu,

$$\psi_{p^2}(x) = \psi_{(2.s+1)^2}(x) \quad = \frac{T_{((2.s+1)^2+1)/2}(x) - T_{((2.s+1)^2-1)/2}(x)}{2^{((2.s+1)^2-1)/2}\left(T_{s+1}(x) - T_s(x)\right)} \tag{3.20}$$

biçimindedir.

İspat. $p > 2$ asal sayı ve $n = p^2$ olsun. $p = 2s + 1$ ($s \in \mathbb{N}$) için Teorem 2.4.1'den $x = \cos(2\pi/p^2)$'nin ψ_{p^2} minimal polinomunun hesabı için (2.3) eşitliği kullanılırsa

$n = (2s + 1)^2 = 2(2s^2 + 2s) + 1$ için

$$T_{2s^2+2s+1}(x) - T_{2s^2+2s}(x) = 2^{2s^2+2s} \prod_{d|p^2} \psi_d(x)$$

$$T_{2s^2+2s+1}(x) - T_{2s^2+2s}(x) = 2^{2s^2+2s} \psi_1(x)\psi_p(x)\psi_{p^2}(x) \tag{3.21}$$

eşitliği alınır. (3.21)'de (3.4) eşitliği göz önüne alınırsa

$$T_{2s^2+2s+1}(x) - T_{2s^2+2s}(x) = 2^{2s^2+2s} \frac{1}{2^s}\left(T_{s+1}(x) - T_s(x)\right)\psi_{p^2}(x)$$

elde edilir. Bu son eşitlikte $\psi_{p^2}(x)$ minimal polinomunun yalnız bırakılması ile istenilen eşitlik

$n = (2s + 1)^2$ için

$$\psi_{p^2}(x) = \psi_{(2.s+1)^2} = \frac{T_{2s^2+2s+1}(x) - T_{2s^2+2s}(x)}{2^{2s^2+s}\left(T_{s+1}(x) - T_s(x)\right)} \tag{3.22}$$

biçiminde elde edilir. Buna ek olarak

$$\psi_{(2.s+1)^2} = \frac{T_{2s^2+2s+1}(x) - T_{2s^2+2s}(x)}{2^{2s^2+s}\left(T_{s+1}(x) - T_s(x)\right)} = \frac{T_{((2.s+1)^2+1)/2}(x) - T_{((2.s+1)^2-1)/2}(x)}{2^{((2.s+1)^2-1)/2}\left(T_{s+1}(x) - T_s(x)\right)}$$

olduğu dikkat edilmelidir.

Aşağıda $n = p^2 \in \mathbb{N}$ olmak üzere $\psi_{p^2}(x)$ minimal polinomunun hesabı için yaptığımız algoritma Teorem 3.2.3.1.'in uygulamasıdır.

$s \in \mathbb{N}$ olmak üzere $\psi_{(2.s+1)^2}(x)$ minimal polinomun hesabı için (3.20) kuralı Maple'da bir döngü içinde ifade edilmelidir. Dikkat edilirse (3.20)'de Chebycheff polinomları bulunmaktadır. Bu polinomların Maple tarafından kolaylıkla hesaplanması için öncelikle " $[G, H, L, P, T, U]$ " isimli paket çağrılmalıdır. Daha sonra da (3.20) kuralı Maple'da sınırlı s değerleri için bir döngü içinde ifade edilmelidir. Artık Maple, asalların kareleri için minimal polinomların genişleyen bir listesini vermeye hazır konumdadır.

Aşağıda (3.20) kuralının Maple'da yapılan algoritmada bir döngü içinde ifade edilişi ve bu döngünün çıktısının liste halinde verilişi görülmektedir. Bu döngüde s değerlerinin üst sınırı istenildiği kadar büyütülebileceğinden bu çalışmada bu liste sadece sınırlı s değerleri için verilmiştir.

```
> with(orthopoly);
```

$$[G, H, L, P, T, U]$$

```
> f:=proc(x)local s,A,B,C;with(orthopoly);for s from 1 to 6
do if isprime(2*s+1) then A:=sort(T(((2*s+1)^2+1)/2,x)-
T(((2*s+1)^2-1)/2,x));B:=sort(T(s+1,x)-
T(s,x));evala(Divide(A,B,'q'));C:=sort(q);print((2*s+1)^2,
sort((1/2)^(((2*s+1)^2-(2*s+1))/2)*C));end if;end do;end
proc;
```

```
f := proc(x)
local s, A, B, C;
    with(orthopoly);
    for s to 6 do
        if isprime(2×s + 1) then
            A := sort(T(1/2×(2×s + 1)^2 + 1/2, x) − T(1/2×(2×s + 1)^2 − 1/2, x))
            ;
            B := sort(T(s + 1, x) − T(s, x));
            evala(Divide(A, B, 'q'));
            C := sort(q);
            print((2×s + 1)^2, sort((1/2)^(1/2×(2×s + 1)^2 − s − 1/2)×C))
        end if
    end do
end proc
```

```
> f(x);
```

$$9,\ x^3-\frac{3}{4}x+\frac{1}{8}$$

$$25,\ x^{10}-\frac{5}{2}x^8+\frac{35}{16}x^6+\frac{1}{32}x^5-\frac{25}{32}x^4-\frac{5}{128}x^3+\frac{25}{256}x^2+\frac{5}{512}x-\frac{1}{1024}$$

$$49,\ x^{21}-\frac{21}{4}x^{19}+\frac{189}{16}x^{17}-\frac{119}{8}x^{15}+\frac{1}{128}x^{14}+\frac{735}{64}x^{13}-\frac{7}{256}x^{12}-\frac{5733}{1024}x^{11}+\frac{77}{2048}x^{10}$$
$$+\frac{7007}{4096}x^9-\frac{105}{4096}x^8-\frac{5147}{16384}x^7+\frac{147}{16384}x^6+\frac{259}{8192}x^5-\frac{49}{32768}x^4-\frac{371}{262144}x^3$$
$$+\frac{49}{524288}x^2+\frac{7}{524288}x-\frac{1}{2097152}$$

$$121,\ x^{55}-\frac{55}{4}x^{53}+\frac{715}{8}x^{51}-\frac{23375}{64}x^{49}+\frac{67375}{64}x^{47}-\frac{582659}{256}x^{45}+\frac{1}{2048}x^{44}$$
$$+\frac{1962015}{512}x^{43}-\frac{11}{2048}x^{42}-\frac{84366645}{16384}x^{41}+\frac{451}{16384}x^{40}+\frac{367982175}{65536}x^{39}-\frac{715}{8192}x^{38}$$
$$-\frac{1317269525}{262144}x^{37}+\frac{100529}{524288}x^{36}+\frac{1949558897}{524288}x^{35}-\frac{162393}{524288}x^{34}-\frac{4793336957}{2097152}x^{33}$$
$$+\frac{1598289}{4194304}x^{32}+\frac{19619239607}{16777216}x^{31}-\frac{191301}{524288}x^{30}-\frac{33417385705}{67108864}x^{29}$$
$$+\frac{9246215}{33554432}x^{28}+\frac{23636685567}{134217728}x^{27}-\frac{5547729}{33554432}x^{26}-\frac{55309822425}{1073741824}x^{25}$$
$$+\frac{21211905}{268435456}x^{24}+\frac{6647803965}{536870912}x^{23}-\frac{258048959}{8589934592}x^{22}-\frac{10414139065}{4294967296}x^{21}$$
$$+\frac{310465133}{34359738368}x^{20}+\frac{820915425}{2147483648}x^{19}-\frac{292746091}{137438953472}x^{18}-\frac{13133636571}{274877906944}x^{17}$$
$$+\frac{53321367}{137438953472}x^{16}+\frac{2551056431}{549755813888}x^{15}-\frac{29417905}{549755813888}x^{14}$$
$$-\frac{749754357}{2199023255552}x^{13}+\frac{47797607}{8796093022208}x^{12}+\frac{321503053}{17592186044416}x^{11}$$
$$-\frac{13737009}{35184372088832}x^{10}-\frac{11936749}{17592186044416}x^9+\frac{658603}{35184372088832}x^8$$
$$+\frac{4537511}{281474976710656}x^7-\frac{306977}{562949953421312}x^6-\frac{120571}{562949953421312}x^5$$
$$+\frac{18271}{2251799813685248}x^4+\frac{5489}{4503599627370496}x^3-\frac{363}{9007199254740992}x^2$$
$$-\frac{33}{18014398509481984}x+\frac{1}{36028797018963968}$$

$$
\begin{aligned}
&169, x^{78} - \frac{39}{2} x^{76} + \frac{2925}{16} x^{74} - \frac{35113}{32} x^{72} + \frac{606411}{128} x^{70} - \frac{4012281}{256} x^{68} + \frac{169258817}{4096} x^{66} \\
&\quad + \frac{1}{8192} x^{65} - \frac{730503345}{8192} x^{64} - \frac{65}{32768} x^{63} + \frac{1314906021}{8192} x^{62} + \frac{2015}{131072} x^{61} \\
&\quad - \frac{4004005291}{16384} x^{60} - \frac{19825}{262144} x^{59} + \frac{41688760971}{131072} x^{58} + \frac{556075}{2097152} x^{57} \\
&\quad - \frac{93502743399}{262144} x^{56} - \frac{2958319}{4194304} x^{55} + \frac{363621779885}{1048576} x^{54} + \frac{24819795}{16777216} x^{53} \\
&\quad - \frac{19705288218335}{67108864} x^{52} - \frac{84240585}{33554432} x^{51} + \frac{58324134324755}{268435456} x^{50} + \frac{1884328875}{536870912} x^{49} \\
&\quad - \frac{37802679654649}{268435456} x^{48} - \frac{4396767375}{1073741824} x^{47} + \frac{343882440712733}{4294967296} x^{46} \\
&\quad + \frac{17283292845}{4294967296} x^{45} - \frac{686438430180555}{17179869184} x^{44} - \frac{28805488075}{8589934592} x^{43} \\
&\quad + \frac{1202538433766241}{68719476736} x^{42} + \frac{163593432275}{68719476736} x^{41} - \frac{28863335944443}{4294967296} x^{40} \\
&\quad - \frac{793766949499}{549755813888} x^{39} + \frac{1242118713957979}{549755813888} x^{38} + \frac{1647566693461}{2199023255552} x^{37} \\
&\quad - \frac{2917993021435999}{4398046511104} x^{36} - \frac{1463039223477}{4398046511104} x^{35} + \frac{2984310576915395}{17592186044416} x^{34} \\
&\quad + \frac{555171133075}{4398046511104} x^{33} - \frac{661738128041393}{17592186044416} x^{32} - \frac{2873827017633}{70368744177664} x^{31} \\
&\quad + \frac{506514951012681}{70368744177664} x^{30} + \frac{3159171416687}{281474976710656} x^{29} - \frac{332578470257657}{281474976710656} x^{28} \\
&\quad - \frac{1467532464489}{562949953421312} x^{27} + \frac{743866969521565}{4503599627370496} x^{26} + \frac{4578698208045}{9007199254740992} x^{25} \\
&\quad - \frac{175563670708413}{9007199254740992} x^{24} - \frac{2973173393775}{36028797018963968} x^{23} + \frac{138436551316115}{72057594037927936} x^{22} \\
&\quad + \frac{1590288757005}{144115188075855872} x^{21} - \frac{11250662745751}{72057594037927936} x^{20} \\
&\quad - \frac{345705522045}{288230376151711744} x^{19} + \frac{11871743606359}{1152921504606846976} x^{18} \\
&\quad + \frac{240286948785}{2305843009213693952} x^{17} - \frac{1245677859153}{2305843009213693952} x^{16} \\
&\quad - \frac{4083817231}{576460752303423488} x^{15} + \frac{405458684553}{18446744073709551616} x^{14} \\
&\quad + \frac{13521774841}{36893488147419103232} x^{13} - \frac{49483859945}{73786976294838206464} x^{12} \\
&\quad - \frac{2051360909}{147573952589676412928} x^{11} + \frac{4324257587}{295147905179352825856} x^{10} \\
&\quad + \frac{216422271}{590295810358705651712} x^{9} - \frac{31616351}{147573952589676412928} x^{8} \\
&\quad - \frac{14656655}{2361183241434822606848} x^{7} + \frac{8903427}{4722366482869645213696} x^{6}
\end{aligned}
$$

$$+\frac{556387}{9444732965739290427392}x^5-\frac{157001}{18889465931478580854784}x^4$$
$$-\frac{9061}{37778931862957161709568}x^3+\frac{507}{37778931862957161709568}x^2$$
$$+\frac{39}{151115727451828646838272}x-\frac{1}{302231454903657293676544}$$
$$\vdots$$

3.2.4. $n = 2^k$ için ψ_{2^k} minimal polinomları

$k \in \mathbb{N}$, $k \geq 1$ olmak üzere $n = 2^k$ olsun. Teorem 2.4.1'den $n = 2^k$ çift için $x = cos(2\pi/2^k)$'nın ψ_{2^k} minimal polinomunun hesabı için (2.4) eşitliği kullanılırsa

$n = 2 = 2.2^0$ için
$$T_2(x) - T_0(x) = 2^1 \prod_{d|2} \psi_d(x) \tag{3.23}$$
$$= 2^1 \psi_1(x)\psi_2(x)$$

eşitliği alınır. (3.23)'te $\psi_1(x) = x + 1$ olduğu göz önüne alınır ve $\psi_2(x)$ yalnız bırakılırsa (3.23)

$n = 2$ için
$$\frac{T_2(x)-T_0(x)}{2^1(x+1)} = \psi_2(x) \tag{3.24}$$

şeklinde elde edilir. Benzer şekilde

$n = 2^2 = 2.2^1 = 4$ için
$$T_3(x) - T_1(x) = 2^2 \prod_{d|4} \psi_d(x) \tag{3.25}$$
$$= 2^2 \psi_1(x)\psi_2(x)\psi_4(x)$$

eşitliği alınır. (3.25)'te (3.23) ele alınırsa ve $\psi_4(x)$ yalnız bırakılırsa minimal polinom

$$T_3(x) - T_1(x) = 2^2\left(\tfrac{1}{2}(T_2(x) - T_0(x))\right)\psi_4(x)$$

$n = 2^2$ için
$$\frac{T_3(x)-T_1(x)}{2^1(T_2(x)-T_0(x))} = \psi_4(x) \tag{3.26}$$

biçiminde bulunur. (3.24) ve (3.26) eşitlikleri gibi benzer işlemler yapılırsa

$n = 2^3 = 8$ için
$$T_5(x) - T_4(x) = 2^4 \prod_{d|8} \psi_d(x)$$

$$T_5(x) - T_4(x) = 2^4\psi_1(x)\psi_2(x)\psi_4(x)\psi_8(x) \tag{3.27}$$

eşitliği elde edilir. (3.27)'de (3.25) göz önünde bulundurulur ve $\psi_8(x)$ yalnız bırakılırsa minimal polinom

$$T_5(x) - T_4(x) = 2^4\left(\tfrac{1}{2^2}(T_3(x) - T_1(x))\right)\psi_8(x)$$

$n = 2^3$ için $$\frac{T_5(x)-T_3(x)}{2^2(T_3(x)-T_1(x))} = \psi_8(x)$$

şeklinde bulunur.

İkinin kuvvetleri için benzer işlemler yapılmaya devam edildiğinde

$n = 2^4 = 16$ için $$\frac{T_9(x)-T_7(x)}{2^4(T_5(x)-T_4(x))} = \psi_{16}(x)$$

$n = 2^5 = 32$ için $$\frac{T_{17}(x)-T_{15}(x)}{2^8(T_9(x)-T_7(x))} = \psi_{32}(x)$$

$\vdots$ $\vdots$

belli bir kuralı izleyen eşitliklerin elde edildiği görülür. Bu eşitliklerdeki kuralı aşağıdaki teoremde veriyoruz.

Teorem 3.2.4.1. $s \geq 1$ ve $n = 2^s$ olsun. O zaman $s \in \mathbb{N}$ olmak üzere $\psi_{2^s}(x)$ minimal polinomu,

$$\psi_{2^s}(x) = \frac{T_{(2^s+2)/2}(x)-T_{(2^s-2)/2}(x)}{2^{2^{(s-2)}}(T_{(2^s+4)/4}(x)-T_{(2^s-4)/4}(x))} \tag{3.28}$$

şeklindedir.

İspat. $s \geq 1$ $(s \in \mathbb{N})$ ve $n = 2^s$ olsun. Teorem 2.4.1'den $n = 2^s$ çift için $x = cos(2\pi/2^s)$'nın ψ_{2^s} minimal polinomunun hesabı için (2.4) eşitliği kullanılırsa

$n = 2^s = 2.2^{s-1}$ için $$T_{2^{s-1}+1}(x) - T_{2^{s-1}-1}(x) = 2^{2^{s-1}}\prod_{d|2^s}\psi_d(x)$$

$$T_{2^{s-1}+1}(x) - T_{2^{s-1}-1}(x) = 2^{2^{s-1}}\psi_1(x)\psi_2(x)\psi_{2^2}(x)\ldots\psi_{2^{s-1}}(x)\psi_{2^s}(x) \tag{3.29}$$

eşitliği elde edilir. (3.29)'da $n = 2^{s-1} = 2.2^{s-2}$ için

$$T_{2^{s-2}+1}(x) - T_{2^{s-2}-1}(x) = 2^{2^{s-2}} \psi_1(x)\psi_2(x)\psi_{2^2}(x) \dots \psi_{2^{s-1}}(x)$$

$$\frac{T_{2^{s-2}+1}(x) - T_{2^{s-2}-1}(x)}{2^{2^{s-2}}} = \psi_1(x)\psi_2(x)\psi_{2^2}(x) \dots \psi_{2^{s-1}}(x) \qquad (3.30)$$

eşitliği alınır. (3.30), (3.29)'da yerine konulursa

$$T_{2^{s-1}+1}(x) - T_{2^{s-1}-1}(x) = 2^{2^{s-1}} \left(\frac{T_{2^{s-2}+1}(x) - T_{2^{s-2}-1}(x)}{2^{2^{s-2}}} \right) \psi_{2^s}(x)$$

eşitliği elde edilir ve bu son eşitlikte $\psi_{2^s}(x)$ minimal polinomunun yalnız bırakılması ile istenilen kural

$n = 2^s$ için $$\psi_{2^s}(x) = \frac{T_{2^{s-1}+1}(x) - T_{2^{s-1}-1}(x)}{2^{2^{(s-2)}}\left(T_{2^{s-2}+1}(x) - T_{2^{s-2}-1}(x)\right)}$$

şeklinde bulunur. Bu kuralın biraz daha sadeleştirilmesi ile

$$\psi_{2^s}(x) = \frac{T_{(2^s+2)/2}(x) - T_{(2^s-2)/2}(x)}{2^{2^{(s-2)}}(T_{(2^s+4)/4}(x) - T_{(2^s-4)/4}(x))} = \frac{T_{2^{s-1}+1}(x) - T_{2^{s-1}-1}(x)}{2^{2^{(s-2)}}\left(T_{2^{s-2}+1}(x) - T_{2^{s-2}-1}(x)\right)}$$

biçiminde istenilen eşitlik bulunur.

Aşağıda $n = 2^s (s \in \mathbb{N})$ olmak üzere $\psi_{2^s}(x)$ minimal polinomunun hesabı için yaptığımız algoritma Teorem 3.2.4.1'in uygulamasıdır.

$s \in \mathbb{N}$ için $\psi_{2^s}(x)$ minimal polinomlarının hesabı için (3.28), Maple'da yapılan bir algoritmada bir döngü içinde ifade edilmelidir. (3.28) eşitliğindeki Chebycheff polinomlarının hesabı için Maple'da öncelikle " $[G, H, L, P, T, U]$ " isimli paket çağrılmalıdır. (3.28) kuralının sınırlı s değerleri için döngü içinde ifade edilmesinden sonra artık Maple, ikinin kuvvetlerinin genişleyen bir listesini vermeye hazırdır.

Aşağıda (3.28) kuralının Maple'da yaptığımız algoritamaya ait bir döngü içinde ifade edilişi görülmekte ve bu döngüye ait liste verilmektedir. Yine burada s değerlerinin üst sınırı istenildiği kadar artırılabilir

```
>f:=proc(x)locals;with(orthopoly);print(2,evala(Divide(T(2,
x)-T(0,x),2*(x-1),'q')),q);for   s   from   2   to   8   do
print(2^s,evala(Divide(sort(T((2^s+2)/2,x)-T((2^s-
```

```
2)/2,x)),sort(T((2^s+4)/4,x)-T((2^s-4)/4,x)),'q')),sort((1/2)^(2^(s-2))*q));end do;end proc;
```

$f := \textbf{proc}(x)$
local s;
with(*orthopoly*);
print(2, evala(Divide(T(2, x) − T(0, x), 2×x − 2, 'q')), q);
for s **from** 2 **to** 8 **do** print(2^s, evala(Divide(
sort(T(1/2×2^s + 1, x) − T(1/2×2^s − 1, x)),
sort(T(1/4×2^s + 1, x) − T(1/4×2^s − 1, x)), 'q')),
sort((1/2)^(2^(s − 2))×q))
end do
end proc

```
> f(x);
```

$$2,\ true,\ x+1$$

$$4,\ true,\ x$$

$$8,\ true,\ x^2-\frac{1}{2}$$

$$16,\ true,\ x^4-x^2+\frac{1}{8}$$

$$32,\ true,\ x^8-2\,x^6+\frac{5}{4}\,x^4-\frac{1}{4}\,x^2+\frac{1}{128}$$

$$64,\ true,\ x^{16}-4\,x^{14}+\frac{13}{2}\,x^{12}-\frac{11}{2}\,x^{10}+\frac{165}{64}\,x^8-\frac{21}{32}\,x^6+\frac{21}{256}\,x^4-\frac{1}{256}\,x^2+\frac{1}{32768}$$

$$128,\ true,\ x^{32}-8\,x^{30}+29\,x^{28}-63\,x^{26}+\frac{2925}{32}\,x^{24}-\frac{1495}{16}\,x^{22}+\frac{8855}{128}\,x^{20}-\frac{4807}{128}\,x^{18}$$
$$+\frac{245157}{16384}\,x^{16}-\frac{17765}{4096}\,x^{14}+\frac{29393}{32768}\,x^{12}-\frac{4199}{32768}\,x^{10}+\frac{12597}{1048576}\,x^8-\frac{357}{524288}\,x^6$$
$$+\frac{85}{4194304}\,x^4-\frac{1}{4194304}\,x^2+\frac{1}{2147483648}$$

$$256,\ true,\ x^{64}-16\,x^{62}+122\,x^{60}-590\,x^{58}+\frac{32509}{16}\,x^{56}-\frac{42427}{8}\,x^{54}+\frac{697851}{64}\,x^{52}$$
$$-\frac{1159587}{64}\,x^{50}+\frac{202927725}{8192}\,x^{48}-\frac{57803655}{2048}\,x^{46}+\frac{443161355}{16384}\,x^{44}-\frac{359546005}{16384}\,x^{42}$$
$$+\frac{7937669495}{524288}\,x^{40}-\frac{2334608675}{262144}\,x^{38}+\frac{9378456563}{2097152}\,x^{36}-\frac{4019338527}{2097152}\,x^{34}$$
$$+\frac{751616304549}{1073741824}\,x^{32}-\frac{29161583781}{134217728}\,x^{30}+\frac{61281589105}{1073741824}\,x^{28}-\frac{13546456539}{1073741824}\,x^{26}$$

$$+\frac{800472431 85}{343597383 68}x^{24}-\frac{6116566755}{17179869184}x^{22}+\frac{6116566755}{137438953472}x^{20}-\frac{616197075}{137438953472}x^{18}$$

$$+\frac{6285210165}{17592186044416}x^{16}-\frac{96695541}{4398046511104}x^{14}+\frac{35624673}{35184372088832}x^{12}$$

$$-\frac{1176791}{35184372088832}x^{10}+\frac{840565}{1125899906842624}x^{8}-\frac{5797}{562949953421312}x^{6}$$

$$+\frac{341}{4503599627370496}x^{4}-\frac{1}{4503599627370496}x^{2}+\frac{1}{9223372036854775808}$$

$$\vdots$$

3.2.5. $n = 2^2p$ için ψ_{2^2p} minimal polinomları

$n \in \mathbb{N}$, $p > 2$ asal sayı olsun. Yukarıdaki minimal polinomlarda olduğu gibi Teorem 2.4.1'den $n = 2^2p$ çift olmak üzere ψ_{2^2p} minimal polinomunun hesabı için (2.4) eşitliği kullanılırsa

$n = 2^2.3 = 12 = 2.6$ için $\qquad T_7(x) - T_5(x) = 2^6 \prod_{d|12} \psi_d(x)$

$$T_7(x) - T_5(x) = 2^6\psi_1(x)\psi_2(x)\psi_3(x)\psi_4(x)\psi_6(x)\psi_{12}(x) \tag{3.31}$$

eşitliği alınır. (3.31)'de (3.5) eşitliği ve $x = cos(2\pi/4) = 0$'ın minimal polinomunun $\psi_4(x) = x$ şeklinde olduğu göz önüne alınırsa

$$n = 12 \text{ için} \qquad T_7(x) - T_5(x) = 2^6 x\left(\tfrac{1}{2^3}\big(T_4(x) - T_2(x)\big)\right)\psi_{12}(x) \tag{3.32}$$

eşitliği elde edilir. (3.32)'de $\psi_{12}(x)$'nin yalnız bırakılması ile istenen minimal polinom

$n = 12 = 2.6$ için $\qquad \frac{T_7(x)-T_5(x)}{2^3x\left(\left(T_4(x)-T_2(x)\right)\right)}=\psi_{12}(x)$

biçiminde bulunur. Benzer şekilde

$n = 2^2.5 = 20 = 2.10$ için $\qquad T_{11}(x) - T_9(x) = 2^{10} \prod_{d|20} \psi_d(x)$

$$T_{11}(x) - T_9(x) = 2^{10}\psi_1(x)\psi_2(x)\psi_4(x)\psi_5(x)\psi_{10}(x)\psi_{20}(x) \tag{3.33}$$

eşitliği alınır. (3.33)'te $\psi_4(x) = x$ minimal polinomu ve (3.8) eşitliği kullanıldığında

$n = 20$ için $$T_{11}(x) - T_9(x) = 2^{10}x\left(\frac{1}{2^5}\big(T_6(x) - T_4(x)\big)\right)\psi_{20}(x) \quad (3.34)$$

eşitliği elde edilir. (3.34)'te $\psi_{20}(x)$ yalnız bırakılırsa istenen minimal polinom

$n = 20 = 2.10$ için $$\frac{T_{11}(x)-T_9(x)}{2^5x\big((T_6(x)-T_4(x))\big)}=\psi_{20}(x)$$

şeklinde bulunur.

$n = 2^2p$ için benzer hesaplamalar yapılmaya devam edildiğinde

$n = 2^27 = 28 = 2.14$ için $$\frac{T_{15}(x)-T_{13}(x)}{2^7x\big((T_8(x)-T_6(x))\big)}=\psi_{28}(x)$$

$n = 2^211 = 44 = 2.22$ için $$\frac{T_{23}(x)-T_{21}(x)}{2^{11}x\big((T_{12}(x)-T_{10}(x))\big)}=\psi_{44}(x)$$

$n = 2^213 = 52 = 2.26$ için $$\frac{T_{27}(x)-T_{25}(x)}{2^{13}x\big((T_{14}(x)-T_{12}(x))\big)}=\psi_{52}(x)$$

$\vdots$ $\vdots$

belirli bir kuralı izleyen eşitliklerin elde edildiği görülür. Bu eşitliklerde kuralı aşağıdaki teoremde veriyoruz.

Teorem 3.2.5.1. $n = 2^2p$ ve $p > 2$ asal sayı olsun. O zaman $s \in \mathbb{N}$, $p = 2s + 1$ olmak üzere ψ_{2^2p} minimal polinomu,

$$\psi_{2^2p}=\psi_{2^2(2.s+1)}(x)=\frac{T_{2.(2.s+1)+1}(x)-T_{2.(2.s+1)-1}(x)}{2^{2s+1}x\big((T_{2.s+2}(x)-T_{2.s}(x))\big)} \quad (3.35)$$

biçimindedir.

İspat. $n = 2^2p$ ve $p > 2$ asal sayı olsun. $s \in \mathbb{N}$, $p = 2s + 1$ için teorem 2.4.1'den $n = 2^2p$ çift olmak üzere $x = cos(2\pi/2^2p)$'nın ψ_{2^2p} minimal polinomunun hesabı için (2.4) eşitliği kullanılırsa

$n = 2^2.p = 2^2(2s + 1) = 2(4s + 2)$ için

$$T_{(4s+2)+1}(x) - T_{(4s+2)-1}(x) = 2^{4s+2} \prod_{d|2^2p} \psi_d(x)$$

$$T_{4s+3}(x) - T_{4s+1}(x) = 2^{4s+2}\psi_1(x)\psi_2(x)\psi_4(x)\psi_p(x)\psi_{2p}(x)\psi_{4p}(x) \tag{3.36}$$

eşitliği alınır. (3.36)'da $\psi_4(x) = x$ minimal polinomu ve (3.12) eşitliği kullanıldığında

$$T_{4s+3}(x) - T_{4s+1}(x) = 2^{4s+2}x\left(\frac{1}{2^{2s+1}}\big(T_{2s+2}(x) - T_{2s}(x)\big)\right)\psi_{2^2p}(x)$$

eşitliği elde edilir. Bu son eşitlikte $\psi_{2^2p}(x)$ yalnız bırskılırsa istenilen kural

$$\frac{T_{4s+3}(x)-T_{4s+1}(x)}{2^{2s+1}x\big(T_{2s+2}(x)-T_{2s}(x)\big)} = \psi_{2^2p}(x)$$

olarak bulunur. Bu kuralda

$$\psi_{2^2p}(x) = \psi_{2^2(2s+1)}(x) = \frac{T_{4s+3}(x)-T_{4s+1}(x)}{2^{2s+1}x\big(T_{2s+2}(x)-T_{2s}(x)\big)} = \frac{T_{2.(2.s+1)+1}(x)-T_{2.(2.s+1)-1}(x)}{2^{2s+1}x\big(T_{2.s+2}(x)-T_{2.s}(x)\big)}$$

eşitliğinin olduğu dikkate alınmalıdır.
Aşağıda $s \in \mathbb{N}$ olmak üzere $\psi_{2^2(2.s+1)}(x)$ minimal polinomunun hesabı için yaptığımız algoritma Teorem 3.2.5.1'in uygulamasıdır.

$s \in \mathbb{N}$ için $\psi_{2^2(2.s+1)}(x)$ minimal polinomların hesabı için (3.35) kuralı Maple'da ifade edilmelidir. Böylece istenen minimal polinomlar Maple'da kolaylıkla saniyeler gibi kısa bir sürede elde edilebilir. Öncelikle (3.35)'teki Chebycheff polinomların Maple'da hesabı için " $[G, H, L, P, T, U]$ " isimli paket çağrılmalıdır. (3.35) kuralı sınırlı s değerleri için Maple'da bir döngü içinde ifade edildikten sonra istenen listenin elde edilmesi için Maple hazırdır.

Aşağıda (3.35) kuralının Maple'da bir döngü içinde ifade edilişi ve bu döngüye ait elde edilen liste görülmektedir. Burada bu döngüde s değerlerinin üstten istenildiği kadar artırılabileceği göz önünde bulundurulmalıdır.

```
> f:= proc(x)local s,A,B,C,E;with(orthopoly);for s from 1 to 25 do if isprime(2*s+1) then A:=sort(T(2*(2*s+1)+1,x)-T(2*(2*s+1)-1,x));B:=sort(T(2*s+2,x)-T(2*s,x));C:=expand(x*B);evala(Divide(A,C,'q'));E:=(1/2)^(2*s+1)*q;print(2^2*(2*s+1),E);end if;end do;end proc;
```

```
f := proc(x)
local s, A, B, C, E;
    with(orthopoly);
    for s to 25 do
        if isprime(2×s + 1) then
            A := sort(T(4×s + 3, x) − T(4×s + 1, x));
            B := sort(T(2×s + 2, x) − T(2×s, x));
            C := expand(x×B);
            evala(Divide(A, C, 'q'));
            E := (1/2)^(2×s + 1)×q;
            print(8×s + 4, E)
        end if
    end do
end proc
```

```
> f(x);
```

$$12,\ x^2-\frac{3}{4}$$

$$20,\ x^4-\frac{5}{4}x^2+\frac{5}{16}$$

$$28,\ x^6-\frac{7}{4}x^4+\frac{7}{8}x^2-\frac{7}{64}$$

$$44,\ x^{10}-\frac{11}{4}x^8+\frac{11}{4}x^6-\frac{77}{64}x^4+\frac{55}{256}x^2-\frac{11}{1024}$$

$$52,\ x^{12}-\frac{13}{4}x^{10}+\frac{65}{16}x^8-\frac{39}{16}x^6+\frac{91}{128}x^4-\frac{91}{1024}x^2+\frac{13}{4096}$$

$$68,\ x^{16}-\frac{17}{4}x^{14}+\frac{119}{16}x^{12}-\frac{221}{32}x^{10}+\frac{935}{256}x^8-\frac{561}{512}x^6+\frac{357}{2048}x^4-\frac{51}{4096}x^2+\frac{17}{65536}$$

$$76, x^{18} - \frac{19}{4}x^{16} + \frac{19}{2}x^{14} - \frac{665}{64}x^{12} + \frac{1729}{256}x^{10} - \frac{2717}{1024}x^{8} + \frac{627}{1024}x^{6} - \frac{627}{8192}x^{4} + \frac{285}{65536}x^{2} - \frac{19}{262144}$$

$$92, x^{22} - \frac{23}{4}x^{20} + \frac{115}{8}x^{18} - \frac{1311}{64}x^{16} + \frac{1173}{64}x^{14} - \frac{2737}{256}x^{12} + \frac{2093}{512}x^{10} - \frac{16445}{16384}x^{8} + \frac{9867}{65536}x^{6} - \frac{3289}{262144}x^{4} + \frac{253}{524288}x^{2} - \frac{23}{4194304}$$

$$116, x^{28} - \frac{29}{4}x^{26} + \frac{377}{16}x^{24} - \frac{725}{16}x^{22} + \frac{7337}{128}x^{20} - \frac{51359}{1024}x^{18} + \frac{127281}{4096}x^{16} - \frac{28101}{2048}x^{14} + \frac{140505}{32768}x^{12} - \frac{121771}{131072}x^{10} + \frac{70499}{524288}x^{8} - \frac{6409}{524288}x^{6} + \frac{2639}{4194304}x^{4} - \frac{1015}{67108864}x^{2} + \frac{29}{268435456}$$

$$124, x^{30} - \frac{31}{4}x^{28} + \frac{217}{8}x^{26} - \frac{3627}{64}x^{24} + \frac{10075}{128}x^{22} - \frac{39215}{512}x^{20} + \frac{54901}{1024}x^{18} - \frac{447051}{16384}x^{16} + \frac{330429}{32768}x^{14} - \frac{350455}{131072}x^{12} + \frac{130169}{262144}x^{10} - \frac{130169}{2097152}x^{8} + \frac{20553}{4194304}x^{6} - \frac{3689}{16777216}x^{4} + \frac{155}{33554432}x^{2} - \frac{31}{1073741824}$$

$$148, x^{36} - \frac{37}{4}x^{34} + \frac{629}{16}x^{32} - \frac{407}{4}x^{30} + \frac{5735}{32}x^{28} - \frac{232841}{1024}x^{26} + \frac{878787}{4096}x^{24} - \frac{627705}{4096}x^{22} + \frac{5476185}{65536}x^{20} - \frac{9126975}{262144}x^{18} + \frac{11560835}{1048576}x^{16} - \frac{1374365}{524288}x^{14} + \frac{1924111}{4194304}x^{12} - \frac{1924111}{33554432}x^{10} + \frac{657305}{134217728}x^{8} - \frac{35853}{134217728}x^{6} + \frac{35853}{4294967296}x^{4} - \frac{2109}{17179869184}x^{2} + \frac{37}{68719476736}$$

$$164, x^{40} - \frac{41}{4}x^{38} + \frac{779}{16}x^{36} - \frac{4551}{32}x^{34} + \frac{73185}{256}x^{32} - \frac{53669}{128}x^{30} + \frac{237677}{512}x^{28} - \frac{405449}{1024}x^{26} + \frac{4312503}{16384}x^{24} - \frac{35937525}{262144}x^{22} + \frac{58659315}{1048576}x^{20} - \frac{37328655}{2097152}x^{18} + \frac{73370115}{16777216}x^{16} - \frac{13706505}{16777216}x^{14} + \frac{7614725}{67108864}x^{12} - \frac{1522945}{134217728}x^{10} + \frac{3350479}{4294967296}x^{8} - \frac{591261}{17179869184}x^{6} + \frac{59983}{68719476736}x^{4} - \frac{1435}{137438953472}x^{2} + \frac{41}{1099511627776}$$

$$172, x^{42} - \frac{43}{4}x^{40} + \frac{215}{4}x^{38} - \frac{10621}{64}x^{36} + \frac{90687}{256}x^{34} - \frac{567987}{1024}x^{32} + \frac{168861}{256}x^{30}$$
$$- \frac{1246355}{2048}x^{28} + \frac{7228859}{16384}x^{26} - \frac{16583853}{65536}x^{24} + \frac{7538115}{65536}x^{22} - \frac{173376645}{4194304}x^{20}$$
$$+ \frac{195747825}{16777216}x^{18} - \frac{171655785}{67108864}x^{16} + \frac{14375115}{33554432}x^{14} - \frac{14375115}{268435456}x^{12}$$
$$+ \frac{20764055}{4294967296}x^{10} - \frac{5167525}{17179869184}x^{8} + \frac{206701}{17179869184}x^{6} - \frac{76153}{274877906944}x^{4}$$
$$+ \frac{3311}{1099511627776}x^{2} - \frac{43}{4398046511104}$$

$$188, x^{46} - \frac{47}{4}x^{44} + \frac{517}{8}x^{42} - \frac{14147}{64}x^{40} + \frac{67445}{128}x^{38} - \frac{475969}{512}x^{36} + \frac{1288599}{1024}x^{34}$$
$$- \frac{21906183}{16384}x^{32} + \frac{18536001}{16384}x^{30} - \frac{50404915}{65536}x^{28} + \frac{55309177}{131072}x^{26} - \frac{196096173}{1048576}x^{24}$$
$$+ \frac{140068695}{2097152}x^{22} - \frac{160350135}{8388608}x^{20} + \frac{72886425}{16777216}x^{18} - \frac{830905245}{1073741824}x^{16}$$
$$+ \frac{455657715}{4294967296}x^{14} - \frac{187623765}{17179869184}x^{12} + \frac{28035735}{34359738368}x^{10} - \frac{11593725}{274877906944}x^{8}$$
$$+ \frac{772915}{549755813888}x^{6} - \frac{59455}{2199023255552}x^{4} + \frac{1081}{4398046511104}x^{2} - \frac{47}{70368744177664}$$

$$\vdots$$

Yukarıda $n \in \mathbb{N}$'nin bazı değerleri için belli bir kuralı izleyen ψ_n minimal polinomları kolayca elde edilmiştir. Fakat $n \in \mathbb{N}$ 'nin bazı değerleri için de ψ_n minimal polinomlarının hangi kuralı takip ettiğini bulmak o kadar da kolay değildir. Hatta bazen bu kuralı bulmaya çalışmak yerine ψ_n minimal polinomun kendisini $n \in \mathbb{N}$'nin tek ve çift olma durumuna gore hesaplamak çok daha kolaydır. Bu durum, Ozgur ve arkadaşları (2012a) tarafından çalışılmıştır.

Aşağıda bu durumu anlatan örneğe yer verilmiştir. Bu örnekte yine Maple'a başvurulmuştur ancak yukarıdaki polinomlardan farklı olarak bir kural olmadığından dolayısı ile bir döngü de söz konusu değildir. Sadece Chebycheff polinomlarını hesaplayan " $[G, H, L, P, T, U]$ " isimli paket çağırılmaktadır. Daha sonra da hesaplanılması istenen minimal polinom, Maple'da ifade edilmektedir. Böylece istenilen minimal polinom çok hızlı bir şekilde hesaplanıp çıktı olarak karşımıza çıkmaktadır.

Örnek 3.2.6. $\psi_{200}(x)=?$

$n=200$ çift olduğundan Teorem 2.4.1'den (2.4) eşitliği kullanıldığında

$n=200=2.100$ için $\quad T_{101}(x)-T_{99}(x)=2^{200}\prod_{d|200}\psi_d(x)$

$$T_{101}(x)-T_{99}(x)=2^{100}\psi_1(x)\psi_2(x)\psi_4(x)\psi_5(x)\psi_8(x)\psi_{10}(x)$$
$$\psi_{20}(x)\psi_{25}(x)\psi_{40}(x)\psi_{50}(x)\psi_{100}(x)\psi_{200}(x) \tag{3.37}$$

eşitliği alınır. (3.37) eşitliğinde $n=100=2.50$ için

$$T_{51}(x)-T_{49}(x)=2^{50}\prod_{d|100}\psi_d(x)$$

$$T_{51}(x)-T_{49}(x)=2^{50}\psi_1(x)\psi_2(x)\psi_4(x)\psi_5(x)\psi_{10}(x)$$
$$\psi_{20}(x)\psi_{25}(x)\psi_{50}(x)\psi_{100}(x) \tag{3.38}$$

eşitliği göz önüne alınırsa (3.37) eşitliği,

$$T_{101}(x)-T_{99}(x)=2^{100}\left(\frac{1}{2^{50}}\big(T_{51}(x)-T_{49}(x)\big)\right)\psi_8(x)\psi_{40}(x)\psi_{200}(x) \tag{3.39}$$

biçimindeki eşitliğe dönüşür. (3.39) eşitliğinde son olarak $\psi_8(x)\psi_{40}(x)$ çarpımı bulunmalıdır. Bunun için $n=40$ durumu kullanılırsa

$n=40=2.20$ için $\quad T_{21}(x)-T_{19}(x)=2^{20}\prod_{d|40}\psi_d(x)$

$$T_{21}(x)-T_{19}(x)=2^{20}\psi_1(x)\psi_2(x)\psi_4(x)\psi_5(x)\psi_8(x)\psi_{10}(x)\psi_{20}(x)\psi_{40}(x) \tag{3.40}$$

eşitliği alınır. (3.40)'ta (3.33) göz önüne alındığında

$$T_{21}(x)-T_{19}(x)=2^{20}\left(\frac{1}{2^{10}}\big(T_{11}(x)-T_9(x)\big)\right)\psi_8(x)\psi_{40}(x)$$

eşitliği elde edilir. Böylece istenilen $\psi_8(x)\psi_{40}(x)$ çarpımı

$$\frac{T_{21}(x)-T_{19}(x)}{2^{10}(T_{11}(x)-T_{9}(x))} = \psi_8(x)\psi_{40}(x) \tag{3.41}$$

biçiminde bulunur. (3.41) eşitliği de (3.39)'da ele alındığında

$$T_{101}(x) - T_{99}(x) = 2^{100}\left(\frac{1}{2^{50}}\big(T_{51}(x) - T_{49}(x)\big)\right)\left(\frac{T_{21}(x)-T_{19}(x)}{2^{10}(T_{11}(x)-T_{9}(x))}\right)\psi_{200}(x) \tag{3.42}$$

eşitliği alınır. (3.42)'de $\psi_{200}(x)$'ün yalnız bırakılması ile de istenilen minimal polinom

$$n = 200 \text{ için} \qquad \frac{(T_{101}(x)-T_{99}(x))(T_{11}(x)-T_{9}(x))}{2^{40}(T_{51}(x)-T_{49}(x))(T_{21}(x)-T_{19}(x))} = \psi_{200}(x) \tag{3.43}$$

biçiminde bulunur.

Görüldüğü gibi (3.43)'teki minimal polinomun el ile hesabını yapabilmek oldukça güçtür. El ile hesaplanmaya çalışıldığında da zaman kaybına sebep olacaktır. Bu sebeple $\psi_{200}(x)$ minimal polinomununu Maple ile ifade edilip hesabının yapılması büyük kolaylıklar sağlayacaktır. Öncelikle Chebycheff polinomlarının hesabını yapıldığı " $[G, H, L, P, T, U]$ " isimli paket çağırılmalıdır. Daha sonra da $\psi_{200}(x)$ minimal polinomu Maple'da ifade edilmelidir. Böylece artık Maple, $\psi_{200}(x)$'ü hesaplamaya hazırdır.

Aşağıda $\psi_{200}(x)$'ün Maple'a uygun dille ifade edilişi ve hesaplanışı görülmektedir.

```
> with(orthopoly);
```

$$[G, H, L, P, T, U]$$

```
> PAY:=sort(expand((T(101,x)-T(99,x))*(T(11,x)-T(9,x))));
```

$$\begin{aligned} PAY := {} & 129807421463370690713262408230502 4\, x^{112} \\ & - 3699511511706064685327978634569318 4\, x^{110} \\ & + 51314496297238726172586545753620480 0\, x^{108} \\ & - 461607360169508367178615492018438144 0\, x^{106} \\ & + 3027834164669135054650935474168791040 0\, x^{104} \\ & - 15437369401121683318620437642107630387 2\, x^{102} \\ & + 63685432365195949993923849244395123507 2\, x^{100} \\ & - 218509226147044112206475861754170572800 0\, x^{98} \end{aligned}$$

$$+ 63607316807729281596136348311430889472 00 \quad x^{96}$$
$$- 15946580684834885324556479422590353408000 \quad x^{94}$$
$$+ 34834358605325517052689313298534044270592 \quad x^{92}$$
$$- 66917313594480361991612561457012027686912 \quad x^{90}$$
$$+ 113891923944517469075220765139427708108800 \quad x^{88}$$
$$- 172786139932854425730819300864818864455680 \quad x^{86}$$
$$+ 234831332943882362120802584827788892569600 \quad x^{84}$$
$$- 287096228425883178617444427508716828360704 \quad x^{82}$$
$$+ 316816177225063864163168739837548779536384 \quad x^{80}$$
$$- 316461791182187374348026487095609104793600 \quad x^{78}$$
$$+ 286797194069414764788723542173968519659520 \quad x^{76}$$
$$- 236256234038165349637916263885756694528000 \quad x^{74}$$
$$+ 177171459417151384315619618274160431595520 \quad x^{72}$$
$$- 121088697850453528192909848919504186245120 \quad x^{70}$$
$$+ 75487245092207484709526975490734161920000 \quad x^{68}$$
$$- 42947537757397768814911475285158684262400 \quad x^{66}$$
$$+ 22305594317421771149818622117551276032000 \quad x^{64}$$
$$- 10575554650077560029495318755811012902912 \quad x^{62}$$
$$+ 4576143136592210769596169871857750638592 \quad x^{60}$$
$$- 1806293320916849465713575138135795302400 \quad x^{58}$$
$$+ 649899347602434022637317514425658245120 \quad x^{56}$$
$$- 212931564583421551820598063375004467200 \quad x^{54}$$
$$+ 63448846904816981502849796472701976576 \quad x^{52}$$
$$- 17168497972560721992249734378318462976 \quad x^{50}$$
$$+ 4210904015313241032733157115297792000 \quad x^{48}$$
$$- 934173870644788978407749534403788800 \quad x^{46}$$
$$+ 186989784743897621891462518013952000 \quad x^{44}$$
$$- 33675441678573344272322087727661056 \quad x^{42}$$
$$+ 5438789975485549777524460267503616 \quad x^{40}$$
$$- 784822588661149624455968220774400 \quad x^{38}$$
$$+ 100757614599638371949157485117440 \quad x^{36}$$
$$- 11452852086249714838848457932800 \quad x^{34}$$

$$+ 1146204470566976255705682542592 \; x^{32}$$
$$- 1003555255189348668003393208 32 \; x^{30}$$
$$+ 763012361523067401357230080 0 \; x^{28} - 4994370788429074083191193 60 \; x^{26}$$
$$+ 27859818323315843923968000 \; x^{24} - 1308532265687095883857920 \; x^{22}$$
$$+ 510028621633964815155 20 \; x^{20} - 16207029643737497600 00 \; x^{18}$$
$$+ 4106894729319997 4400 \; x^{16} - 806836471421952000 \; x^{14}$$
$$+ 11842346373288960 \; x^{12} - 123452179023360 \; x^{10} + 849761352000 \; x^{8}$$
$$- 3447021600 \; x^{6} + 6736000 \; x^{4} - 4000 \; x^{2}$$

```
>    PAYDA:=sort(expand((2^40)*((T(51,x)-T(49,x))*(T(21,x)-T(19,x)))));
```

$$PAYDA := 1298074214633706907132624082305024 \; x^{72}$$
$$- 2401437297072357778195354552264294 4 \; x^{70}$$
$$+ 21296530083834253945144613850316800 0 \; x^{68}$$
$$- 12053836027450187732951851439279308 80 \; x^{66}$$
$$+ 48911030759206003227348796476227584 00 \; x^{64}$$
$$- 15152055224046394996891489862223396864 \; x^{62}$$
$$+ 37263942927637196948939038826875060224 \; x^{60}$$
$$- 74692987997030944094231187208064204800 \; x^{58}$$
$$+ 124315921132699197241927067035647344640 \; x^{56}$$
$$- 174152719650649556543364666656974438400 \; x^{54}$$
$$+ 207430763357559264509898352693082062848 \; x^{52}$$
$$- 211653717806671267294508732948674510848 \; x^{50}$$
$$+ 186039877628460178466769074688884736000 \; x^{48}$$
$$- 141432629545461157074997203050063462400 \; x^{46}$$
$$+ 93245088437146403460948198263095296000 \; x^{44}$$
$$- 53396722003839876005775443177200680960 \; x^{42}$$
$$+ 26573871432001918910580349861426626560 \; x^{40}$$
$$- 11488804613469649476698526002970624000 \; x^{38}$$
$$+ 4309271919293772984471633139230310400 \; x^{36}$$
$$- 1399167236196293197343591600488448000 \; x^{34}$$
$$+ 391995261602095003349865517109215232 \; x^{32}$$
$$- 94361496730680700884700642748137472 \; x^{30}$$
$$+ 19411863669722895663043690941644800 \; x^{28}$$
$$- 3389844534357209762141710120386560 \; x^{26}$$

$$+\, 498356215343890537543922352128000\ x^{24}$$
$$-\, 610578650624637706233492956774440\ x^{22}$$
$$+\, 615704183937918857684413579264 0\ x^{20}$$
$$-\, 503196183387225101214679040000\ x^{18}$$
$$+\, 32693722066568586870967500800\ x^{16}$$
$$-\, 164779897094790181185126400 0\ x^{14} + 62401294110154774502440960\ x^{12}$$
$$-\, 1700903480080115024527360\ x^{10} + 31404594160165978112000\ x^{8}$$
$$-\, 357804833129470361600\ x^{6} + 2128654511374336000\ x^{4}$$
$$-\, 4398046511104000\ x^{2}$$

```
> evala(Divide(PAY,PAYDA,'q'));
```

$$true$$

```
> PSI200:=sort(q);
```

$$PSI200 := x^{40} - 10\, x^{38} + \frac{185}{4} x^{36} - \frac{525}{4} x^{34} + \frac{32725}{128} x^{32} - \frac{5797}{16} x^{30} + \frac{49445}{128} x^{28}$$
$$- \frac{40455}{128} x^{26} + \frac{13147875}{65536} x^{24} - \frac{3251625}{32768} x^{22} + \frac{40060019}{1048576} x^{20} - \frac{11930095}{1048576} x^{18}$$
$$+ \frac{5432435}{2097152} x^{16} - \frac{116075}{262144} x^{14} + \frac{14855725}{268435456} x^{12} - \frac{1306503}{268435456} x^{10} + \frac{1221495}{4294967296} x^{8}$$
$$- \frac{21615}{2147483648} x^{6} + \frac{12475}{68719476736} x^{4} - \frac{75}{68719476736} x^{2} + \frac{1}{1099511627776}$$

3.3. P_q^* Minimal Polinomlarının Maple ile Hesaplanışı

$q \in \mathbb{N}$, $q > 3$ olmak üzere $x = 2cos(\pi/q)$'nun P_q^* minimal polinomunun MAPLE ile hesabı Cangül (1993)'ün çalışması temel alınırak yapılmıştır. Buna göre Cangül (1993) çalışmasında q'nun tek ve çift olduğu durumlarda P_q^*'ın förmüllerini vermiş ve $1 \le q \le 50$ için P_q^*'nun bir listesini de oldukça uzun süren bir zaman sonucunda verebilmeyi başarmıştır. Bu tez çalışmasının bu bölümünde Cangül'ün bu çalışmasına ek olarak $q > 50$ için hesaplanması çok güç olan ve uzun süren P_q^*'ın daha da genişleyen bir listesinin, kolaylıkla ve çok kısa süren bir zamanda MAPLE'da yazılan algoritmalar tarafından elde edildiği görülmüştür. Burada ψ_n polinomlarında olduğu gibi belli özellikteki $q \in \mathbb{N}$, $q > 3$ sayıları için belli gruplar oluşturulmuştur. Daha sonra da oluşturulan her bir gruba ilişkin P_q^*'ın hesabı için kurallar geliştirilmiştir. Son olarak bu kurallar MAPLE'a bir döngü içinde ifade edilmiştir. Böylece bu döngü ile istenilen P_q^*

minimal polinomların genişleyen bir listesi, kolaylıkla ve saniyeler gibi kısa süren bir zaman diliminde hızlı bir şekilde Maple tarafından verilir.

$q \in \mathbb{N}$, $q > 3$ sayılarının içinde belli bir özelliğe sahip sayılar olduğu gibi belli bir özelliğe uymayan sayılarda vardır. Bu durumda bu tür sayılara ilişkin P_q^* minimal polinomları için kural geliştirmek güç olduğundan bu polinomların hesabı için Cangül (1993)'ün çalışmasında q tek ve çift için elde edilen P_q^* formüllerine başvurulur. Dikkat edilirse bu förmüllerde P_q^*, Dickson polinomları, Euler fonksiyonu ve ψ_{2n} minimal poinomlarına bağlıdır. Dolayısı ile P_q^*'in MAPLE ile hesabı için Dickson polinomları, Euler fonksiyonu ve ψ_{2n} minimal poinomları MAPLE'da ifade edilir. Böylece q'nun çok büyük değerleri için hesaplanması güç olan ve çok zaman alan bir P_q^* minimial polinomu MAPLE ile kolaylıkla saniyeler içinde hesap edilip bulunur.

Aşağıda belli özellikteki $q \in \mathbb{N}$, $q \geq 3$ sayıları için oluşturulan bazı P_q^* minimial polinom gruplarının MAPLE ile hesaplanışı anlatılmaktadır. Bu durum Ozgur ve arkadaşları (2012c) tarafından çalışılmıştır.

3.3.1. $q = p$ için P_p^* minimal polinomları

$q \in \mathbb{N}$, $q = p \geq 3$ asal olsun. Teorem 2.5.3'ten $q = p$ tek olmak üzere $\lambda_p = 2cos(\pi/p)$'nun P_p^* minimal polinomunun hesabı için (2.5) eşitliği kullanılırsa

$p = 3$ için
$$P_3^*(x) = 2^{\frac{\varphi(3)-3-1}{2}} . \frac{D_2(x)+D_1(x)}{\prod_{\substack{d|6 \\ d\neq 6 \\ d\,çift}} \psi_d(x/2)} \tag{3.44}$$

eşitliği alınır. (3.44)'te $\varphi(3) = 2$ ve çarpım sembolü altındaki $d|6$, $d \neq 6$, d çift koşulları için d böleni 2 olup

$$\prod_{\substack{d|6 \\ d\neq 6 \\ d\,çift}} \psi_d(x/2) = \psi_2(x/2)$$

eşitliği geçerli olur. Böylece

$p = 3$ için
$$P_3^*(x) = 2^{-1} . \frac{D_2(x)+D_1(x)}{\psi_2(x/2)}$$

minimal polinomu elde edilir. Benzer şekilde

$p = 5$ için $$P_5^*(x) = 2^{-1}.\frac{D_3(x)+D_2(x)}{\prod_{\substack{d|10 \\ d\neq 10 \\ d\,çift}} \psi_d(x/2)} \tag{3.45}$$

eşitliği alınır. (3.45)'te çarpım sembolü altındaki $d|10$, $d \neq 10$, d çift koşulları için d böleni 2 olup

$$\prod_{\substack{d|10 \\ d\neq 10 \\ d\,çift}} \psi_d(x/2) = \psi_2(x/2)$$

eşitliği elde edilir. Son olarak istenen minimal polinom

$p = 5$ için $$P_5^*(x) = 2^{-1}.\frac{D_3(x)+D_2(x)}{\psi_2(x/2)}$$

biçiminde bulunur. Bu şekilde devam edilirse

$p = 7$ için $$P_7^*(x) = 2^{-1}.\frac{D_4(x)+D_3(x)}{\psi_2(x/2)}$$

$p = 11$ için $$P_{11}^*(x) = 2^{-1}.\frac{D_5(x)+D_4(x)}{\psi_2(x/2)}$$

$p = 13$ için $$P_{13}^*(x) = 2^{-1}.\frac{D_3(x)+D_2(x)}{\psi_2(x/2)}$$

$\vdots$ $\vdots$

asallar için belli kuralı izleyen eşitliklerin ortaya çıktığı görülür. Buna göre bu eşitliklerde $k \in \mathbb{N}$, $2k+1$ asal olmak üzere

$p = 2k+1$ için $$P_{2k+1}^*(x) = 2^{-1}.\frac{D_{k+1}(x)+D_k(x)}{\psi_2(x/2)} \tag{3.46}$$

kuralı geçerlidir. Son olarak $n = 2$ için $x/2 = \cos(2\pi/2) = -1$ olmak üzere $\psi_2(x/2) = (x+2)/2$'dir . Bu eşitlik (3.46)'da kullanılırsa $k \in \mathbb{N}$ olmak üzere

$p = 2k + 1$ için $$P^*_{2k+1}(x) = 2^{-1}.\frac{D_{k+1}(x)+D_k(x)}{2^{-1}(x+2)}$$

$p = 2k + 1$ için $$P^*_{2k+1}(x) = \frac{D_{k+1}(x)+D_k(x)}{x+2}$$

biçiminde çok basit bir kural elde edilir. Bu kuralı aşağıdaki teorem ile veriyoruz.

Teorem 3.3.1.1. $q = p$ ve $p \geq 3$ asal sayı olsun. O zaman $k \geq 1$ $(k \in \mathbb{N})$, $p = 2k + 1$ olmak üzere P^*_p minimal polinomu,

$$P^*_p = P^*_{2k+1}(x) = \frac{D_{k+1}(x)+D_k(x)}{x+2} \tag{3.47}$$

şeklindedir.

İspat. $q = p \geq 3$ asal sayı olsun. Teorem 2.5.3'ten $q = p$ tek olmak üzere $\lambda_p = 2cos(\pi/p)$'nun P^*_p minimal polinomunun hesabı için (2.5) eşitliği kullanılırsa

$q = p$ için $$P^*_p(x) = 2^{\frac{\varphi(p)-p-1}{2}}.\frac{D_{(p+1)/2}(x)+D_{(p-1)/2}(x)}{\prod_{\substack{d|2p \\ d\neq 2p \\ d\ çift}} \psi_d(x/2)} \tag{3.48}$$

eşitliği alınır. (3.48)'de çarpım sembolü altındaki $d|2p$'nin d bölenleri: 1, 2, p, 2p'dir. $d \neq 2p$ ve $d\ çift$ koşulları için d böleni 2 olup çarpım sembolu için

$$\prod_{\substack{d|2p \\ d\neq 2p \\ d\ çift}} \psi_d(x/2) = \psi_2(x/2) = (x+2)/2$$

eşitliği elde edilir. Bu son eşitlik ve $\varphi(p) = p - 1$ olduğu (3.48)'de göz önüne alınırsa istenen minimal polinom,

$q = p = 2k + 1$ için $\qquad P_p^*(x) = 2^{\frac{p-1-p-1}{2}} . \frac{D_{(p+1)/2}(x)+D_{(p-1)/2}(x)}{2^{-1}(x+2)}$

$$P_p^*(x) = P_{2k+1}^*(x) = \frac{D_{k+1}(x)+D_k(x)}{x+2}$$

olarak bulunur.

Aşağıda $q = p$ asal olmak üzere P_p^*'nin hesabı için yazılan algoritma teorem 3.3.1.1'in uygulamasıdır.

$q = p$ asal olmak üzere P_p^*'nin hesabı için (3.47)'de elde edilen kural MAPLE'da bir döngü içinde ifade edilmelidir. Dikkat edilirse bu kural, Dickson polinomlarına bağlıdır. Dolayısı ile bu döngüdeki Dickson polinomları, (2.2)'deki tanım kullanılarak Maple dilinde anlatılmalıdır. Böylece istenen asal minimal polinomların bir listesi, MAPLE tarafından verilir.

Aşağıda Maple'da (3.47)'ye ait algoritma ve bu algoritmaya ait liste verilmektedir. Bu algoritmadaki döngünün üst sınırı istenildiği kadar artırılabilineceğinden bu çalışmada bu döngü, $0 \leq k \leq 50$ için sınırlandırılmıştır.

```
> f:=proc(x)local k,A,B,C,P;for k from 0 to 50 do if
isprime(2*k+1) then A:=sort(sum((-1)^i*(k+1)*(k-i)!/(k+1-
2*i)!*1/i!*x^(k+1-2*i),i=0..floor((k+1)/2)));B:=sort(sum((-
1)^i*k*(k-1-i)!/(k-2*i)!*1/i!*x^(k-2*i),i=0..floor(k/2)));
C:=sort(A+B);evala(Divide(C,x+2,'Q'));P:=sort(Q);
print(2*k+1,P);end if; end do;end proc;
```

```
f := proc(x)
local k, A, B, C, P;
    for k from 0 to 50 do
        if isprime(2×k + 1) then
            A := sort(sum(
```

```
            (-1)^i×(k+1)×(k-i)!×x^(k+1-2×i)/((k+1-2×i)!×i!),
            i = 0 .. floor(1/2×k+1/2)));
        B := sort(sum((-1)^i×k×(k-1-i)!×x^(k-2×i)/((k-2×i)!×i!),
            i = 0 .. floor(1/2×k)));
        C := sort(A+B);
        evala(Divide(C, x+2, 'Q')); end proc
        P := sort(Q);
        print(2×k+1, P)
    end if
end do
```

```
> f(x);
```

$$3, x-1$$

$$5, x^2-x-1$$

$$7, x^3-x^2-2x+1$$

$$11, x^5-x^4-4x^3+3x^2+3x-1$$

$$13, x^6-x^5-5x^4+4x^3+6x^2-3x-1$$

$$17, x^8-x^7-7x^6+6x^5+15x^4-10x^3-10x^2+4x+1$$

$$19, x^9-x^8-8x^7+7x^6+21x^5-15x^4-20x^3+10x^2+5x-1$$

$$23, x^{11}-x^{10}-10x^9+9x^8+36x^7-28x^6-56x^5+35x^4+35x^3-15x^2-6x+1$$

$$29, x^{14}-x^{13}-13x^{12}+12x^{11}+66x^{10}-55x^9-165x^8+120x^7+210x^6-126x^5 -126x^4+56x^3+28x^2-7x-1$$

$$31, x^{15}-x^{14}-14x^{13}+13x^{12}+78x^{11}-66x^{10}-220x^9+165x^8+330x^7-210x^6 -252x^5+126x^4+84x^3-28x^2-8x+1$$

$$37, x^{18}-x^{17}-17x^{16}+16x^{15}+120x^{14}-105x^{13}-455x^{12}+364x^{11}+1001x^{10}-715x^9 -1287x^8+792x^7+924x^6-462x^5-330x^4+120x^3+45x^2-9x-1$$

$$41, x^{20}-x^{19}-19x^{18}+18x^{17}+153x^{16}-136x^{15}-680x^{14}+560x^{13}+1820x^{12} -1365x^{11}-3003x^{10}+2002x^9+3003x^8-1716x^7-1716x^6+792x^5+495x^4 -165x^3-55x^2+10x+1$$

$$43, x^{21}-x^{20}-20x^{19}+19x^{18}+171x^{17}-153x^{16}-816x^{15}+680x^{14}+2380x^{13} -1820x^{12}-4368x^{11}+3003x^{10}+5005x^9-3003x^8-3432x^7+1716x^6+1287x^5 -495x^4-220x^3+55x^2+11x-1$$

$47, x^{23} - x^{22} - 22\,x^{21} + 21\,x^{20} + 210\,x^{19} - 190\,x^{18} - 1140\,x^{17} + 969\,x^{16} + 3876\,x^{15} - 3060\,x^{14} - 8568\,x^{13} + 6188\,x^{12} + 12376\,x^{11} - 8008\,x^{10} - 11440\,x^{9} + 6435\,x^{8} + 6435\,x^{7} - 3003\,x^{6} - 2002\,x^{5} + 715\,x^{4} + 286\,x^{3} - 66\,x^{2} - 12\,x + 1$

$53, x^{26} - x^{25} - 25\,x^{24} + 24\,x^{23} + 276\,x^{22} - 253\,x^{21} - 1771\,x^{20} + 1540\,x^{19} + 7315\,x^{18} - 5985\,x^{17} - 20349\,x^{16} + 15504\,x^{15} + 38760\,x^{14} - 27132\,x^{13} - 50388\,x^{12} + 31824\,x^{11} + 43758\,x^{10} - 24310\,x^{9} - 24310\,x^{8} + 11440\,x^{7} + 8008\,x^{6} - 3003\,x^{5} - 1365\,x^{4} + 364\,x^{3} + 91\,x^{2} - 13\,x - 1$

$59, x^{29} - x^{28} - 28\,x^{27} + 27\,x^{26} + 351\,x^{25} - 325\,x^{24} - 2600\,x^{23} + 2300\,x^{22} + 12650\,x^{21} - 10626\,x^{20} - 42504\,x^{19} + 33649\,x^{18} + 100947\,x^{17} - 74613\,x^{16} - 170544\,x^{15} + 116280\,x^{14} + 203490\,x^{13} - 125970\,x^{12} - 167960\,x^{11} + 92378\,x^{10} + 92378\,x^{9} - 43758\,x^{8} - 31824\,x^{7} + 12376\,x^{6} + 6188\,x^{5} - 1820\,x^{4} - 560\,x^{3} + 105\,x^{2} + 15\,x - 1$

$61, x^{30} - x^{29} - 29\,x^{28} + 28\,x^{27} + 378\,x^{26} - 351\,x^{25} - 2925\,x^{24} + 2600\,x^{23} + 14950\,x^{22} - 12650\,x^{21} - 53130\,x^{20} + 42504\,x^{19} + 134596\,x^{18} - 100947\,x^{17} - 245157\,x^{16} + 170544\,x^{15} + 319770\,x^{14} - 203490\,x^{13} - 293930\,x^{12} + 167960\,x^{11} + 184756\,x^{10} - 92378\,x^{9} - 75582\,x^{8} + 31824\,x^{7} + 18564\,x^{6} - 6188\,x^{5} - 2380\,x^{4} + 560\,x^{3} + 120\,x^{2} - 15\,x - 1$

$67, x^{33} - x^{32} - 32\,x^{31} + 31\,x^{30} + 465\,x^{29} - 435\,x^{28} - 4060\,x^{27} + 3654\,x^{26} + 23751\,x^{25} - 20475\,x^{24} - 98280\,x^{23} + 80730\,x^{22} + 296010\,x^{21} - 230230\,x^{20} - 657800\,x^{19} + 480700\,x^{18} + 1081575\,x^{17} - 735471\,x^{16} - 1307504\,x^{15} + 817190\,x^{14} + 1144066\,x^{13} - 646646\,x^{12} - 705432\,x^{11} + 352716\,x^{10} + 293930\,x^{9} - 125970\,x^{8} - 77520\,x^{7} + 27132\,x^{6} + 11628\,x^{5} - 3060\,x^{4} - 816\,x^{3} + 136\,x^{2} + 17\,x - 1$

$71, x^{35} - x^{34} - 34\,x^{33} + 33\,x^{32} + 528\,x^{31} - 496\,x^{30} - 4960\,x^{29} + 4495\,x^{28} + 31465\,x^{27} - 27405\,x^{26} - 142506\,x^{25} + 118755\,x^{24} + 475020\,x^{23} - 376740\,x^{22} - 1184040\,x^{21} + 888030\,x^{20} + 2220075\,x^{19} - 1562275\,x^{18} - 3124550\,x^{17} + 2042975\,x^{16} + 3268760\,x^{15} - 1961256\,x^{14} - 2496144\,x^{13} + 1352078\,x^{12} + 1352078\,x^{11} - 646646\,x^{10} - 497420\,x^{9} + 203490\,x^{8} + 116280\,x^{7} - 38760\,x^{6} - 15504\,x^{5} + 3876\,x^{4} + 969\,x^{3} - 153\,x^{2} - 18\,x + 1$

$73, x^{36} - x^{35} - 35\,x^{34} + 34\,x^{33} + 561\,x^{32} - 528\,x^{31} - 5456\,x^{30} + 4960\,x^{29} + 35960\,x^{28} - 31465\,x^{27} - 169911\,x^{26} + 142506\,x^{25} + 593775\,x^{24} - 475020\,x^{23} - 1560780\,x^{22} + 1184040\,x^{21} + 3108105\,x^{20} - 2220075\,x^{19} - 4686825\,x^{18} + 3124550\,x^{17} + 5311735\,x^{16} - 3268760\,x^{15} - 4457400\,x^{14} + 2496144\,x^{13} + 2704156\,x^{12} - 1352078\,x^{11} - 1144066\,x^{10} + 497420\,x^{9} + 319770\,x^{8} - 116280\,x^{7} - 54264\,x^{6} + 15504\,x^{5} + 4845\,x^{4} - 969\,x^{3} - 171\,x^{2} + 18\,x + 1$

$79, x^{39} - x^{38} - 38\ x^{37} + 37\ x^{36} + 666\ x^{35} - 630\ x^{34} - 7140\ x^{33} + 6545\ x^{32} + 52360\ x^{31}$
$- 46376\ x^{30} - 278256\ x^{29} + 237336\ x^{28} + 1107568\ x^{27} - 906192\ x^{26} - 3365856\ x^{25}$
$+ 2629575\ x^{24} + 7888725\ x^{23} - 5852925\ x^{22} - 14307150\ x^{21} + 10015005\ x^{20}$
$+ 20030010\ x^{19} - 13123110\ x^{18} - 21474180\ x^{17} + 13037895\ x^{16} + 17383860\ x^{15}$
$- 9657700\ x^{14} - 10400600\ x^{13} + 5200300\ x^{12} + 4457400\ x^{11} - 1961256\ x^{10}$
$- 1307504\ x^{9} + 490314\ x^{8} + 245157\ x^{7} - 74613\ x^{6} - 26334\ x^{5} + 5985\ x^{4} + 1330\ x^{3}$
$- 190\ x^{2} - 20\ x + 1$

$83, x^{41} - x^{40} - 40\ x^{39} + 39\ x^{38} + 741\ x^{37} - 703\ x^{36} - 8436\ x^{35} + 7770\ x^{34} + 66045\ x^{33}$
$- 58905\ x^{32} - 376992\ x^{31} + 324632\ x^{30} + 1623160\ x^{29} - 1344904\ x^{28} - 5379616\ x^{27}$
$+ 4272048\ x^{26} + 13884156\ x^{25} - 10518300\ x^{24} - 28048800\ x^{23} + 20160075\ x^{22}$
$+ 44352165\ x^{21} - 30045015\ x^{20} - 54627300\ x^{19} + 34597290\ x^{18} + 51895935\ x^{17}$
$- 30421755\ x^{16} - 37442160\ x^{15} + 20058300\ x^{14} + 20058300\ x^{13} - 9657700\ x^{12}$
$- 7726160\ x^{11} + 3268760\ x^{10} + 2042975\ x^{9} - 735471\ x^{8} - 346104\ x^{7} + 100947\ x^{6}$
$+ 33649\ x^{5} - 7315\ x^{4} - 1540\ x^{3} + 210\ x^{2} + 21\ x - 1$

$89, x^{44} - x^{43} - 43\ x^{42} + 42\ x^{41} + 861\ x^{40} - 820\ x^{39} - 10660\ x^{38} + 9880\ x^{37} + 91390\ x^{36}$
$- 82251\ x^{35} - 575757\ x^{34} + 501942\ x^{33} + 2760681\ x^{32} - 2324784\ x^{31}$
$- 10295472\ x^{30} + 8347680\ x^{29} + 30260340\ x^{28} - 23535820\ x^{27} - 70607460\ x^{26}$
$+ 52451256\ x^{25} + 131128140\ x^{24} - 92561040\ x^{23} - 193536720\ x^{22}$
$+ 129024480\ x^{21} + 225792840\ x^{20} - 141120525\ x^{19} - 206253075\ x^{18}$
$+ 119759850\ x^{17} + 145422675\ x^{16} - 77558760\ x^{15} - 77558760\ x^{14} + 37442160\ x^{13}$
$+ 30421755\ x^{12} - 13037895\ x^{11} - 8436285\ x^{10} + 3124550\ x^{9} + 1562275\ x^{8}$
$- 480700\ x^{7} - 177100\ x^{6} + 42504\ x^{5} + 10626\ x^{4} - 1771\ x^{3} - 253\ x^{2} + 22\ x + 1$

$97, x^{48} - x^{47} - 47\ x^{46} + 46\ x^{45} + 1035\ x^{44} - 990\ x^{43} - 14190\ x^{42} + 13244\ x^{41} + 135751\ x^{40}$
$- 123410\ x^{39} - 962598\ x^{38} + 850668\ x^{37} + 5245786\ x^{36} - 4496388\ x^{35}$
$- 22481940\ x^{34} + 18643560\ x^{33} + 76904685\ x^{32} - 61523748\ x^{31} - 211915132\ x^{30}$
$+ 163011640\ x^{29} + 472733756\ x^{28} - 348330136\ x^{27} - 854992152\ x^{26}$
$+ 600805296\ x^{25} + 1251677700\ x^{24} - 834451800\ x^{23} - 1476337800\ x^{22}$
$+ 927983760\ x^{21} + 1391975640\ x^{20} - 818809200\ x^{19} - 1037158320\ x^{18}$
$+ 565722720\ x^{17} + 601080390\ x^{16} - 300540195\ x^{15} - 265182525\ x^{14}$
$+ 119759850\ x^{13} + 86493225\ x^{12} - 34597290\ x^{11} - 20030010\ x^{10} + 6906900\ x^{9}$
$+ 3108105\ x^{8} - 888030\ x^{7} - 296010\ x^{6} + 65780\ x^{5} + 14950\ x^{4} - 2300\ x^{3} - 300\ x^{2}$
$+ 24\ x + 1$

$$
\begin{aligned}
101,\; & x^{50} - x^{49} - 49\,x^{48} + 48\,x^{47} + 1128\,x^{46} - 1081\,x^{45} - 16215\,x^{44} + 15180\,x^{43} \\
& + 163185\,x^{42} - 148995\,x^{41} - 1221759\,x^{40} + 1086008\,x^{39} + 7059052\,x^{38} \\
& - 6096454\,x^{37} - 32224114\,x^{36} + 26978328\,x^{35} + 118030185\,x^{34} - 95548245\,x^{33} \\
& - 350343565\,x^{32} + 273438880\,x^{31} + 847660528\,x^{30} - 635745396\,x^{29} \\
& - 1676056044\,x^{28} + 1203322288\,x^{27} + 2707475148\,x^{26} - 1852482996\,x^{25} \\
& - 3562467300\,x^{24} + 2310789600\,x^{23} + 3796297200\,x^{22} - 2319959400\,x^{21} \\
& - 3247943160\,x^{20} + 1855967520\,x^{19} + 2203961430\,x^{18} - 1166803110\,x^{17} \\
& - 1166803110\,x^{16} + 565722720\,x^{15} + 471435600\,x^{14} - 206253075\,x^{13} \\
& - 141120525\,x^{12} + 54627300\,x^{11} + 30045015\,x^{10} - 10015005\,x^{9} - 4292145\,x^{8} \\
& + 1184040\,x^{7} + 376740\,x^{6} - 80730\,x^{5} - 17550\,x^{4} + 2600\,x^{3} + 325\,x^{2} - 25\,x - 1
\end{aligned}
$$

$$\vdots$$

3.3.2. $q = 2p$ için P_{2p}^* minimal polinomları

$q \in \mathbb{N}$, $q = 2p \geq 3$ ve $p > 2$ asal olsun. Teorem 2.5.5'ten $q = 2p$ çift olmak üzere $\lambda_p = 2cos(\pi/2p)$'nin P_{2p}^* minimal polinomunun hesabı için (2.6) eşitliği kullanılırsa

$q = 2.3 = 6$ için
$$P_6^*(x) = 2^{\frac{\varphi(12)-6}{2}} . \frac{D_7(x) - D_5(x)}{\prod_{\substack{d|12 \\ d \neq 12 \\ d \nmid 6}} \psi_d\left(\frac{x}{2}\right) . [D_4(x) - D_2(x)]} \tag{3.49}$$

eşitliği alınır. (3.49)'da $\varphi(12) = \varphi(3)\varphi(2^2) = 2.2 = 4$'tür. $d|12$'nin d bölenleri: 1, 2, 3, 4, 6, 12'dir. $d \neq 12$ ve $d \nmid 6$ koşulları için d bölenleri: 4'tür. O halde (3.49)'da $\psi_4(x) = x$ olmak üzere çarpım sembolü için

$$\prod_{\substack{d|12 \\ d \neq 12 \\ d \nmid 6}} \psi_d(x/2) = \psi_4(x/2) = x/2 \tag{3.50}$$

eşitliği elde edilir. (3.50), (3.49)'da kullanılırsa minimal polinom

$q = 2.3 = 6$ için
$$P_6^*(x) = \frac{D_7(x) - D_5(x)}{x[D_4(x) - D_2(x)]}$$

biçiminde bulunur. Benzer şekilde

$q = 2.5 = 10$ için $$P^*_{10}(x) = 2^{\frac{\varphi(20)-6}{2}} \cdot \frac{D_{11}(x) - D_9(x)}{\prod_{\substack{d|20 \\ d\neq 20 \\ d\nmid 10}} \psi_d\left(\frac{x}{2}\right) \cdot [D_6(x) - D_4(x)]} \tag{3.51}$$

eşitliği bulunur. (3.51)'de $\varphi(20) = \varphi(5)\varphi(2^2) = 4.2 = 8$'tür. $d|20$'nin d bölenleri: 1, 2, 4, 5, 10, 20'dir. $d \neq 20$ ve $d \nmid 10$ koşulları için d bölenleri sadece 4'tür. O halde (3.51)'de $\psi_4(x) = x$ olmak üzere çarpım sembolü için

$$\prod_{\substack{d|20 \\ d\neq 20 \\ d\nmid 10}} \psi_d(x/2) = \psi_4(x/2) = x/2 \tag{3.52}$$

eşitliği geçerlidir. (3.52), (3.51)'de ele alınırsa

$q = 2.5 = 10$ için $$P^*_{10}(x) = \frac{D_{11}(x) - D_9(x)}{x[D_6(x) - D_4(x)]}$$

eşitliği elde edilir. Bu şekilde devam edildiğinde

$q = 2.7 = 14$ için $$P^*_{10}(x) = \frac{D_{15}(x) - D_{13}(x)}{x[D_8(x) - D_6(x)]}$$

$q = 2.11 = 22$ için $$P^*_{22}(x) = \frac{D_{23}(x) - D_{22}(x)}{x[D_{12}(x) - D_{10}(x)]}$$

$q = 2.13 = 26$ için $$P^*_{22}(x) = \frac{D_{27}(x) - D_{25}(x)}{x[D_{14}(x) - D_{12}(x)]}$$

$\vdots$ $\qquad\qquad$ $\vdots$

biçiminde belli bir kuralı izleyen eşitlikler ortaya çıkar. Bu eşitliklerdeki kuralı aşağıdaki teoremde veriyoruz.

Teorem 3.3.2.1. $q = 2p \geq 3$ ve $p > 2$ asal sayı olsun. O zaman $k \in \mathbb{N}$, $p = 2k + 1$ olmak üzere P^*_{2p} minimal polinomu,

$$P^*_{2p} = P^*_{2(2k+1)}(x) = \frac{D_{(4k+3/2)}(x) - D_{(4k+1/2)}(x)}{x[D_{2k+2}(x) - D_{2k}(x)]} \tag{3.53}$$

biçimindedir.

İspat. $q \in \mathbb{N}$, $q = 2p \geq 3$ ve $p > 2$ asal sayı olsun. Yardımcı teorem 2.7.2.a. ve 2.7.2.b. gereğince P_{2p}^* minimal polinomu için

$$P_{2p}^*(x) = \frac{D_{2p+1}(x) - D_{2p-1}(x)}{x\left(D_{p+1}(x) - D_{p-1}(x)\right)}$$

eşitliği alınır. Böylece bu eşitlik ile istenilen kural $k \in \mathbb{N}$ olmak üzere

$p = 2k + 1$ için $$P_{2(2k+1)}^*(x) = \frac{D_{4k+3}(x) - D_{4k+1}(x)}{x\left(D_{(2k+2}(x) - D_{2k}(x)\right)}$$

biçiminde elde edilir.

Aşağıda $q = 2p$ için P_{2p}^* minimal polinomunun hesabı için yazılan algoritma teorem 3.3.2.1'in uygulamasıdır.

$q = 2p$ için P_{2p}^* minimal polinomunun kolay ve hızlı bir şekilde hesaplanamabilmesi için (3.53)'teki kural MAPLE'da bir döngü içinde ifade edilmelidir. Bu kural, Dickson polinomlarına bağlıdır. Dolayısı ile bu döngüdeki Dickson polinomları, (2.2)'deki tanım kullanılarak Maple'a anlatılmalıdır. Böylece asalın iki katı biçimindeki minimal polinomların genişleyen bir listesi çok kısa bir sürede Maple'da yazılan algoritma tarafından verilir.

Aşağıda (3.53) kuralına ilişkin algoritma ve bu algoritmaya ait liste verilmiştir. Yine bu algoritmadaki döngünün üst sınırı istenilenildiği kadar artırılabilineceğinden bu çalışmada bu döngü $1 \leq k \leq 40$ için sınırlandırılmıştır.

```
> f:=proc(x)local  k,A,B,E,F,PAY,PAYDA,MINPOL;for  k  from  1
to    40    do    if    isprime(2*k+1)    then    A:=sort(sum((-
1)^i*(4*k+3)*(4*k+2-i)!/(4*k+3-2*i)!*1/i!*x^(4*k+3-
2*i),i=0..(2*k+1)));B:=sort(sum((-1)^i*(4*k+1)*(4*k-
i)!/(4*k+1-2*i)!*1/i!*x^(4*k+1-
2*i),i=0..2*k));E:=sort(sum((-1)^i*(2*k+2)*(2*k+1-
i)!/(2*k+2-2*i)!*1/i!*x^(2*k+2-
```

```
2*i),i=0..(k+1)));F:=sort(sum((-1)^i*2*k*(2*k-1-i)!/(2*k-
2*i)!*1/i!*x^(2*k-2*i),i=0..k));PAY:=sort(A-B);PAYDA:=x*(E-
F);evala(Divide(PAY,PAYDA,'q'));MINPOL:=sort(q);print(2*(2*
k+1),MINPOL);end if;end do;end proc;
```

$f := \mathbf{proc}(x)$

local $k, A, B, E, F, PAY, PAYDA, MINPOL;$

for k **to** 40 **do**

if isprime$(2\times k+1)$ **then**

$A :=$ sort(sum($(\text{-}1)$^$i\times(4\times k+3)\times(4\times k+2-i)!\times x$^$(4\times k+3-2\times i)/((4\times k+3-2\times i)!\times i!), i=0..2\times k+1$));

$B :=$ sort(sum($(\text{-}1)$^$i\times(4\times k+1)\times(4\times k-i)!\times x$^$(4\times k+1-2\times i)/((4\times k+1-2\times i)!\times i!), i=0..2\times k$));

$E :=$ sort(sum($(\text{-}1)$^$i\times(2\times k+2)\times(2\times k+1-i)!\times x$^$(2\times k+2-2\times i)/((2\times k+2-2\times i)!\times i!), i=0..k+1$));

$F :=$ sort(sum($2\times(\text{-}1)$^$i\times k\times(2\times k-1-i)!\times x$^$(2\times k-2\times i)/((2\times k-2\times i)!\times i!), i=0..k$));

$PAY :=$ sort$(A-B)$;

$PAYDA := x\times(E-F)$;

evala(Divide($PAY, PAYDA, 'q'$)); **end proc**

$MINPOL :=$ sort(q);

print$(4\times k+2, MINPOL)$

end if

end do

> `f(x);`

$$6, x^2-3$$

$$10, x^4-5x^2+5$$

$$14, x^6-7x^4+14x^2-7$$

$$22, x^{10}-11x^8+44x^6-77x^4+55x^2-11$$

$$26, x^{12}-13x^{10}+65x^8-156x^6+182x^4-91x^2+13$$

$$34, x^{16}-17x^{14}+119x^{12}-442x^{10}+935x^8-1122x^6+714x^4-204x^2+17$$

$$38, x^{18}-19x^{16}+152x^{14}-665x^{12}+1729x^{10}-2717x^8+2508x^6-1254x^4+285x^2-19$$

$$46, x^{22}-23x^{20}+230x^{18}-1311x^{16}+4692x^{14}-10948x^{12}+16744x^{10}-16445x^8+9867x^6-3289x^4+506x^2-23$$

$58, x^{28} - 29\,x^{26} + 377\,x^{24} - 2900\,x^{22} + 14674\,x^{20} - 51359\,x^{18} + 127281\,x^{16} - 224808\,x^{14}$
$+ 281010\,x^{12} - 243542\,x^{10} + 140998\,x^{8} - 51272\,x^{6} + 10556\,x^{4} - 1015\,x^{2} + 29$

$62, x^{30} - 31\,x^{28} + 434\,x^{26} - 3627\,x^{24} + 20150\,x^{22} - 78430\,x^{20} + 219604\,x^{18} - 447051\,x^{16}$
$+ 660858\,x^{14} - 700910\,x^{12} + 520676\,x^{10} - 260338\,x^{8} + 82212\,x^{6} - 14756\,x^{4}$
$+ 1240\,x^{2} - 31$

$74, x^{36} - 37\,x^{34} + 629\,x^{32} - 6512\,x^{30} + 45880\,x^{28} - 232841\,x^{26} + 878787\,x^{24}$
$- 2510820\,x^{22} + 5476185\,x^{20} - 9126975\,x^{18} + 11560835\,x^{16} - 10994920\,x^{14}$
$+ 7696444\,x^{12} - 3848222\,x^{10} + 1314610\,x^{8} - 286824\,x^{6} + 35853\,x^{4} - 2109\,x^{2} + 37$

$82, x^{40} - 41\,x^{38} + 779\,x^{36} - 9102\,x^{34} + 73185\,x^{32} - 429352\,x^{30} + 1901416\,x^{28}$
$- 6487184\,x^{26} + 17250012\,x^{24} - 35937525\,x^{22} + 58659315\,x^{20} - 74657310\,x^{18}$
$+ 73370115\,x^{16} - 54826020\,x^{14} + 30458900\,x^{12} - 12183560\,x^{10} + 3350479\,x^{8}$
$- 591261\,x^{6} + 59983\,x^{4} - 2870\,x^{2} + 41$

$86, x^{42} - 43\,x^{40} + 860\,x^{38} - 10621\,x^{36} + 90687\,x^{34} - 567987\,x^{32} + 2701776\,x^{30}$
$- 9970840\,x^{28} + 28915436\,x^{26} - 66335412\,x^{24} + 120609840\,x^{22} - 173376645\,x^{20}$
$+ 195747825\,x^{18} - 171655785\,x^{16} + 115000920\,x^{14} - 57500460\,x^{12}$
$+ 20764055\,x^{10} - 5167525\,x^{8} + 826804\,x^{6} - 76153\,x^{4} + 3311\,x^{2} - 43$

$94, x^{46} - 47\,x^{44} + 1034\,x^{42} - 14147\,x^{40} + 134890\,x^{38} - 951938\,x^{36} + 5154396\,x^{34}$
$- 21906183\,x^{32} + 74144004\,x^{30} - 201619660\,x^{28} + 442473416\,x^{26}$
$- 784384692\,x^{24} + 1120549560\,x^{22} - 1282801080\,x^{20} + 1166182800\,x^{18}$
$- 830905245\,x^{16} + 455657715\,x^{14} - 187623765\,x^{12} + 56071470\,x^{10} - 11593725\,x^{8}$
$+ 1545830\,x^{6} - 118910\,x^{4} + 4324\,x^{2} - 47$

$106, x^{52} - 53\,x^{50} + 1325\,x^{48} - 20776\,x^{46} + 229172\,x^{44} - 1890669\,x^{42} + 12108327\,x^{40}$
$- 61669740\,x^{38} + 253873763\,x^{36} - 853939021\,x^{34} + 2363226593\,x^{32}$
$- 5401660784\,x^{30} + 10210456360\,x^{28} - 15944020316\,x^{26} + 20499454692\,x^{24}$
$- 21578373360\,x^{22} + 18443677230\,x^{20} - 12657425550\,x^{18} + 6871173870\,x^{16}$
$- 2893125840\,x^{14} + 920540040\,x^{12} - 213696795\,x^{10} + 34467225\,x^{8} - 3596580\,x^{6}$
$+ 217035\,x^{4} - 6201\,x^{2} + 53$

$118, x^{58} - 59\,x^{56} + 1652\,x^{54} - 29205\,x^{52} + 365859\,x^{50} - 3455335\,x^{48} + 25556440\,x^{46}$
$- 151794020\,x^{44} + 736647450\,x^{42} - 2956411766\,x^{40} + 9894929176\,x^{38}$
$- 27773267119\,x^{36} + 65592184047\,x^{34} - 130526252535\,x^{32} + 218786861392\,x^{30}$
$- 308290577416\,x^{28} + 363854576834\,x^{26} - 357739373862\,x^{24}$
$+ 290845019400\,x^{22} - 193641552390\,x^{20} + 104268528210\,x^{18} - 44686512090\,x^{16}$
$+ 14932102320\,x^{14} - 3787127400\,x^{12} + 703323660\,x^{10} - 91018356\,x^{8}$
$+ 7637904\,x^{6} - 371287\,x^{4} + 8555\,x^{2} - 59$

$122, x^{60} - 61\ x^{58} + 1769\ x^{56} - 32452\ x^{54} + 422730\ x^{52} - 4160871\ x^{50} + 32152185\ x^{48}$
$- 200058040\ x^{46} + 1020107270\ x^{44} - 4315838450\ x^{42} + 15283145570\ x^{40}$
$- 45571561336\ x^{38} + 114858935204\ x^{36} - 245179650147\ x^{34} + 443410005585\ x^{32}$
$- 678610095504\ x^{30} + 876538040026\ x^{28} - 951535947194\ x^{26}$
$+ 863020975362\ x^{24} - 648887951400\ x^{22} + 400411345620\ x^{20}$
$- 200205672810\ x^{18} + 79802261190\ x^{16} - 24835486320\ x^{14} + 5873256900\ x^{12}$
$- 1018031196\ x^{10} + 123058716\ x^{8} - 9651664\ x^{6} + 438712\ x^{4} - 9455\ x^{2} + 61$

$134, x^{66} - 67\ x^{64} + 2144\ x^{62} - 43617\ x^{60} + 633485\ x^{58} - 6992857\ x^{56} + 60986884\ x^{54}$
$- 431264394\ x^{52} + 2518145487\ x^{50} - 12301285425\ x^{48} + 50758988280\ x^{46}$
$- 178150864710\ x^{44} + 534452594130\ x^{42} - 1374959237890\ x^{40}$
$+ 3038993463800\ x^{38} - 5774087581220\ x^{36} + 9425348845815\ x^{34}$
$- 13195488384141\ x^{32} + 15798679970128\ x^{30} - 16110496022170\ x^{28}$
$+ 13916726351066\ x^{26} - 10113397410402\ x^{24} + 6129331763880\ x^{22}$
$- 3064665881940\ x^{20} + 1247247742650\ x^{18} - 406246407606\ x^{16}$
$+ 103657619952\ x^{14} - 20155648324\ x^{12} + 2879378332\ x^{10} - 287415260\ x^{8}$
$+ 18643152\ x^{6} - 701624\ x^{4} + 12529\ x^{2} - 67$

$142, x^{70} - 71\ x^{68} + 2414\ x^{66} - 52327\ x^{64} + 812240\ x^{62} - 9613968\ x^{60} + 90223392\ x^{58}$
$- 689161713\ x^{56} + 4364690849\ x^{54} - 23231419035\ x^{52} + 104960312886\ x^{50}$
$- 405528481605\ x^{48} + 1347179362620\ x^{46} - 3862867084860\ x^{44}$
$+ 9584557428600\ x^{42} - 20606798471490\ x^{40} + 38403578969595\ x^{38}$
$- 61997934676405\ x^{36} + 86563154076490\ x^{34} - 104261288816825\ x^{32}$
$+ 107941099010360\ x^{30} - 95604973409176\ x^{28} + 72014135814704\ x^{26}$
$- 45791597230002\ x^{24} + 24357232569150\ x^{22} - 10717182330426\ x^{20}$
$+ 3847193657076\ x^{18} - 1107525446734\ x^{16} + 250205084312\ x^{14}$
$- 43138807640\ x^{12} + 5471263408\ x^{10} - 485354012\ x^{8} + 28001193\ x^{6} - 937839\ x^{4}$
$+ 14910\ x^{2} - 71$

$146, x^{72} - 73\ x^{70} + 2555\ x^{68} - 57086\ x^{66} + 914617\ x^{64} - 11190608\ x^{62} + 108732624\ x^{60}$
$- 861388320\ x^{58} + 5668597752\ x^{56} - 31413479209\ x^{54} + 148092116271\ x^{52}$
$- 598448493318\ x^{50} + 2084759095575\ x^{48} - 6286350503580\ x^{46}$
$+ 16454103860460\ x^{44} - 37447270854840\ x^{42} + 74155450837545\ x^{40}$
$- 127746785056275\ x^{38} + 191233066114545\ x^{36} - 248267489341690\ x^{34}$
$+ 278715388977935\ x^{32} - 269526969561080\ x^{30} + 223404707390200\ x^{28}$
$- 157743149913776\ x^{26} + 94163002754652\ x^{24} - 47081501377326\ x^{22}$
$+ 19495286167698\ x^{20} - 6592608848980\ x^{18} + 1789422401866\ x^{16}$
$- 381444273752\ x^{14} + 62095579448\ x^{12} - 7440023344\ x^{10} + 623782445\ x^{8}$
$- 34024497\ x^{6} + 1077699\ x^{4} - 16206\ x^{2} + 73$

$158, x^{78} - 79\, x^{76} + 3002\, x^{74} - 73075\, x^{72} + 1280274\, x^{70} - 17197194\, x^{68} + 184221996\, x^{66}$
$- 1616328703\, x^{64} + 11837900360\, x^{62} - 73394982232\, x^{60} + 389312514448\, x^{58}$
$- 1781052706472\, x^{56} + 7071045073456\, x^{54} - 24476694485040\, x^{52}$
$+ 74129417583264\, x^{50} - 196906265455545\, x^{48} + 459447952729605\, x^{46}$
$- 942434984631315\, x^{44} + 1699472923105650\, x^{42} - 2692322893972635\, x^{40}$
$+ 3741872496707730\, x^{38} - 4552918752151770\, x^{36} + 4836114655395660\, x^{34}$
$- 4468149409876425\, x^{32} + 3574519527901140\, x^{30} - 2462446785887452\, x^{28}$
$+ 1451020892700008\, x^{26} - 725510446350004\, x^{24} + 304836321995800\, x^{22}$
$- 106377364779224\, x^{20} + 30393532794064\, x^{18} - 6985610359926\, x^{16}$
$+ 1263355065093\, x^{14} - 174772439835\, x^{12} + 17819935042\, x^{10} - 1272852503\, x^{8}$
$+ 59202442\, x^{6} - 1600066\, x^{4} + 20540\, x^{2} - 79$

3.3.3. $q = p^2$ için $P^*_{p^2}$ minimal polinomları

$q \in \mathbb{N}$, $q = p^2 \geq 3$ ve $p > 2$ asal sayı olsun. Teorem 2.5.3'ten $q = p^2$ tek olmak üzere $\lambda_{p^2} = 2cos(\pi/p^2)$ 'nin $P^*_{p^2}$ 'nin minimal polinomunun hesabı için (2.5) eşitliği kullanılırsa

$q = 3^2 = 9$ için
$$P^*_9(x) = 2^{\frac{\varphi(9)-9-1}{2}} . \frac{D_5(x)+D_4(x)}{\prod_{\substack{d|18 \\ d \neq 18 \\ d\, çift}} \psi_d(x/2)} \tag{3.54}$$

eşitliği elde edilir. Bu eşitlikte $\varphi(9) = \varphi(3^2) = 3^2 - 3^1 = 6$ ve $d|18$'in d bölenleri:1, 2, 3, 6, 9, 18 olup $d \neq 18$, d çift koşulları için d bölenleri: 2 ve 6'dır. Buna göre (3.54)'te çarpım sembolü için

$$\prod_{\substack{d|18 \\ d \neq 18 \\ d\, çift}} \psi_d(x/2) = \psi_2(x/2)\psi_6(x/2) \tag{3.55}$$

eşitliği geçerlidir. (3.55), (3.54)'te düşünüldüğünde son olarak minimal polinom

$q = 3^2 = 9$ için
$$P^*_9(x) = 2^{-2}\, \frac{D_5(x)+D_4(x)}{\psi_2(x/2)\psi_6(x/2)}$$

biçiminde bulunur. Benzer şekilde

$q = 5^2 = 25$ için $$P_9^*(x) = 2^{\frac{\varphi(25)-25-1}{2}} . \frac{D_{13}(x)+D_{12}(x)}{\prod_{\substack{d|50 \\ d\neq 50 \\ d\, çift}} \psi_d(x/2)} \tag{3.56}$$

eşitliği alınır. Bu eşitlikte $\varphi(25) = \varphi(5^2) = 5^2 - 5^1 = 20$ ve $d|50$'in d bölenleri 1, 2, 5, 10, 25, 50 olup $d \neq 50$, d çift koşulları için d bölenleri 2 ve 10'dur. Buna göre (3.56)'daki çarpım sembolü için

$$\prod_{\substack{d|50 \\ d\neq 50 \\ d\, çift}} \psi_d(x/2) = \psi_2(x/2)\psi_{10}(x/2) \tag{3.57}$$

eşitliği geçerli olur. (3.57), (3.56)'da ele alındığında minimal polinom

$q = 5^2 = 25$ için $$P_9^*(x) = 2^{-3} . \frac{D_{13}(x)+D_{12}(x)}{\psi_2(x/2)\psi_{10}(x/2)}$$

şeklinde alınır. Bu şekilde yapılmaya devam edildiğinde

$q = 7^2 = 49$ için $$P_{49}^*(x) = 2^{-4} . \frac{D_{35}(x)+D_{24}(x)}{\psi_2(x/2)\psi_{14}(x/2)}$$

$q = 11^2 = 121$ için $$P_{121}^*(x) = 2^{-6} . \frac{D_{61}(x)+D_{60}(x)}{\psi_2(x/2)\psi_{22}(x/2)}$$

$q = 13^2 = 169$ için $$P_{169}^*(x) = 2^{-7} . \frac{D_{85}(x)+D_{84}(x)}{\psi_2(x/2)\psi_{26}(x/2)}$$

⋮ ⋮

belli kuralı takip eden eşitlikler bulunur. Bu eşitliklerdeki kuralı aşağıdaki teoermde veriyoruz.

Teorem 3.3.3.1. $q = p^2 \geq 3$ ve $p > 2$ asal sayı olsun. O zaman $k \in \mathbb{N}$, $p = 2k + 1$ olmak üzere $P_{p^2}^*$ minimal polinomu,

$$P^*_{p^2} = P^*_{(2k+1)^2}(x) = 2^{-(k+1)}.\frac{D_{2k^2+2k+1}(x)+D_{2k^2+2k}(x)}{\psi_2(x/2)\psi_{2(2k+1)}(x/2)} \tag{3.58}$$

biçimindedir.

İspat. $q \in \mathbb{N}$, $q = p^2 \geq 3$ ve $p > 2$ asal olsun. Teorem 2.5.3'ten $q = p^2$ olmak üzere $\lambda_{p^2} = 2cos(\pi/p^2)$ 'nin $P^*_{p^2}$ 'nin minimal polinomunun hesabı için (2.5) eşitliği kullanılırsa

$q = p^2$ için
$$P^*_{p^2}(x) = 2^{\frac{\varphi(p^2)-p^2-1}{2}}.\frac{D_{(p^2+1)/2}(x)+D_{(p^2-1)/2}(x)}{\prod_{\substack{d|2p^2 \\ d\neq 2p^2 \\ d\, çift}} \psi_d(x/2)} \tag{3.59}$$

eşitliği alınır. (3.59)'da $\varphi(p^2) = p^2 - p$'dir ve çarpım sembolü altındaki $d|2p^2$'nin d bölenleri $1, 2, p, 2p, p^2, 2p^2$ olup $d \neq 2p^2$ ve $d\; çift$ koşulları için bu bölenler 2 ve $2p$'dir. Böylece (3.59)'daki çarpım sembolü için

$$\prod_{\substack{d|2p^2 \\ d\neq 2p^2 \\ d\, çift}} \psi_d(x/2) = \psi_2(x/2)\psi_{2p}(x/2) \tag{3.60}$$

eşitliği geçerli olur. (3.60), (3.59)'da ele alındığında minimal polinom

$q = p^2$ için
$$P^*_{p^2}(x) = 2^{\frac{-p-1}{2}}.\frac{D_{(p^2+1)/2}(x)+D_{(p^2-1)/2}(x)}{\psi_2(x/2)\psi_{2p}(x/2)} \tag{3.61}$$

şeklini alır.

(3.61)'de (3.10) ve $\psi_2(x/2) = (x+2)/2$ kullanılırsa $k \in \mathbb{N}$ olmak üzere istenilen minimal polinom

$q = p^2 = (2k+1)^2 = 4k^2 + 4k + 1$ için

$$P^*_{(2k+1)^2}(x) = 2^{\frac{-(2k+1)-1}{2}}.\frac{D_{(4k^2+4k+2)/2}(x)+D_{(4k^2+4k)/2}(x)}{2^{-1}(x+2)\left(\frac{T_{2k+2}(x)-T_{2k}(x)}{2^{s+1}(x+1)\left(T_{k+1}(x)-T_k(x)\right)}\right)}$$

$$P^*_{p^2} = P^*_{(2k+1)^2}(x) = 2^{-(k+1)} . \frac{D_{2k^2+2k+1}(x)+D_{2k^2+2k}(x)}{2^{-1}(x+2)\left(\frac{T_{2k+2}(x)-T_{2k}(x)}{2^{k+1}(x+1)\left(T_{k+1}(x)-T_k(x)\right)}\right)} \tag{3.62}$$

şeklini alır.

Aşağıda verilen algoritma $q = p^2$ için $P^*_{p^2}$ minimal polinomununun hesabı için teorem 3.3.3.1'in uygulamasıdır.

$q = p^2$ için $P^*_{p^2}$ minimal polinomununun MAPLE'da hızlı bir şekilde hesaplanabilmesi için (3.62) kuralı MAPLE'da bir döngü içinde ifade edilmelidir. (3.62) kuralı önceki minimal polinomlardan farklı olarak ψ_n'lere de bağlıdır. Dolayısı ile ψ_{2p}'ye ait döngüye, $P^*_{p^2}$ minimal polinomlarının hesaplanması için oluşturulan döngüde ihtiyaç duyulacaktır. Yine benzer olarak bu döngüde Dickson polinomları da yer alacağından (2.2)'deki tanım kullanılarak Dickson polinomları, bu döngü içinde MAPLE'a anlatılacaktır. $q = p^2$ için $P^*_{p^2}$ minimal polinomuna ait döngü için yapılan hazırlıkların sonunda MAPLE, $P^*_{p^2}$ minimal polinomlarının genişleyen bir listesini vermeye hazır konumdadır.

Aşağıda $q = p^2$ için $P^*_{p^2}$ minimal polinomuna ait algoritma ve bu algoritmaya ait çıktı görülmektedir. Bu döngü $k \in \mathbb{N}$ olmak üzere $1 \leq k \leq 10$ için sınırlandırılmıştır. k istenildiği kadar artırılıp istenildiği kadar uzun bir liste elde edilebilir.

```
> f:=proc(x)local k,A,B,C,F,E,G,H,K,L,P;with(orthopoly);for
k from 0 to 10 do if isprime(2*k+1) then A:=sort(sum((-
1)^i*(2*k^2+2*k+1)*(2*k^2+2*k-i)!/(2*k^2+2*k+1-
2*i)!*1/i!*x^(2*k^2+2*k+1-
2*i),i=0..floor((4*k^2+4*k+2)/4)));B:=sort(sum((-
1)^i*(2*k^2+2*k)*(2*k^2+2*k-1-i)!/(2*k^2+2*k-
2*i)!*1/i!*x^(2*k^2+2*k-
2*i),i=0..floor(k^2+k)));C:=sort(A+B);F:=sort(T(2*k+2,x)-
T(2*k,x));E:=sort(T(k+1,x)-
T(k,x));G:=expand((x+1)*E);evala(Divide(F,G,'q'));H:=((1/2)
^(k+1))*q;K:=subs(x=x/2,H);L:=1/2*(x+2)*K;;evala(Divide(C,L
```

```
,'q1'));P:=sort((1/2)^(k+1)*q1);print((2*k+1)^2,P);end
if;end do;end proc;
```

f := **proc**(x)
local $k, A, B, C, F, E, G, H, K, L, P$;
with($orthopoly$);
for k **from** 0 **to** 10 **do**
if isprime($2 \times k + 1$) **then**
A := sort(sum((-1)^i×(2×k^2 + 2×k + 1)×(2×k^2 + 2×k − i)!×
x^(2×k^2 + 2×k + 1 − 2×i)/((2×k^2 + 2×k + 1 − 2×i)!×i!),
i = 0 .. floor(k^2 + k + 1/2)));
B := sort(sum((-1)^i×(2×k^2 + 2×k)×(2×k^2 + 2×k − 1 − i)!×
x^(2×k^2 + 2×k − 2×i)/((2×k^2 + 2×k − 2×i)!×i!),
i = 0 .. floor(k^2 + k)));
C := sort($A + B$);
F := sort(T(2×k + 2, x) − T(2×k, x));
E := sort(T(k + 1, x) − T(k, x));
G := expand((x + 1)×E);
evala(Divide(F, G, 'q'));
H := (1/2)^(k + 1)×q;
K := subs(x = 1/2×x, H);
L := 1/2×(x + 2)×K;
evala(Divide(C, L, '$q1$'));
P := sort((1/2)^(k + 1)×$q1$);
print((2×k + 1)^2, P)
end if
end do
end proc

```
> f(x);
```

$$9, x^3 - 3x - 1$$

$$25, x^{10} - 10x^8 + 35x^6 - x^5 - 50x^4 + 5x^3 + 25x^2 - 5x - 1$$

$$49, x^{21} - 21x^{19} + 189x^{17} - 952x^{15} - x^{14} + 2940x^{13} + 14x^{12} - 5733x^{11} - 77x^{10} + 7007x^9 + 210x^8 - 5147x^7 - 294x^6 + 2072x^5 + 196x^4 - 371x^3 - 49x^2 + 14x + 1$$

$121, x^{55} - 55\, x^{53} + 1430\, x^{51} - 23375\, x^{49} + 269500\, x^{47} - 2330636\, x^{45} - x^{44}$
$+ 15696120\, x^{43} + 44\, x^{42} - 84366645\, x^{41} - 902\, x^{40} + 367982175\, x^{39} + 11440\, x^{38}$
$- 1317269525\, x^{37} - 100529\, x^{36} + 3899117794\, x^{35} + 649572\, x^{34} - 9586673914\, x^{33}$
$- 3196578\, x^{32} + 19619239607\, x^{31} + 12243264\, x^{30} - 33417385705\, x^{29}$
$- 36984860\, x^{28} + 47273371134\, x^{27} + 88763664\, x^{26} - 55309822425\, x^{25}$
$- 169695240\, x^{24} + 53182431720\, x^{23} + 258048959\, x^{22} - 41656556260\, x^{21}$
$- 310465133\, x^{20} + 26269293600\, x^{19} + 292746091\, x^{18} - 13133636571\, x^{17}$
$- 213285468\, x^{16} + 5102112862\, x^{15} + 117671620\, x^{14} - 1499508714\, x^{13}$
$- 47797607\, x^{12} + 321503053\, x^{11} + 13737009\, x^{10} - 47746996\, x^{9} - 2634412\, x^{8}$
$+ 4537511\, x^{7} + 306977\, x^{6} - 241142\, x^{5} - 18271\, x^{4} + 5489\, x^{3} + 363\, x^{2} - 33\, x - 1$

$169, x^{78} - 78\, x^{76} + 2925\, x^{74} - 70226\, x^{72} + 1212822\, x^{70} - 16049124\, x^{68} + 169258817\, x^{66}$
$- x^{65} - 1461006690\, x^{64} + 65\, x^{63} + 10519248168\, x^{62} - 2015\, x^{61} - 64064084656\, x^{60}$
$+ 39650\, x^{59} + 333510087768\, x^{58} - 556075\, x^{57} - 1496043894384\, x^{56}$
$+ 5916638\, x^{55} + 5817948478160\, x^{54} - 49639590\, x^{53} - 19705288218335\, x^{52}$
$+ 336962340\, x^{51} + 58324134324755\, x^{50} - 1884328875\, x^{49}$
$- 151210718618596\, x^{48} + 8793534750\, x^{47} + 343882440712733\, x^{46}$
$- 34566585690\, x^{45} - 686438430180555\, x^{44} + 115221952300\, x^{43}$
$+ 1202538433766241\, x^{42} - 327186864550\, x^{41} - 1847253500444352\, x^{40}$
$+ 793766949499\, x^{39} + 2484237427915958\, x^{38} - 1647566693461\, x^{37}$
$- 2917993021435999\, x^{36} + 2926078446954\, x^{35} + 2984310576915395\, x^{34}$
$- 4441369064600\, x^{33} - 2646952512165572\, x^{32} + 5747654035266\, x^{31}$
$+ 2026059804050724\, x^{30} - 6318342833374\, x^{29} - 1330313881030628\, x^{28}$
$+ 5870129857956\, x^{27} + 743866969521565\, x^{26} - 4578698208045\, x^{25}$
$- 351127341416826\, x^{24} + 2973173393775\, x^{23} + 138436551316115\, x^{22}$
$- 1590288757005\, x^{21} - 45002650983004\, x^{20} + 691411044090\, x^{19}$
$+ 11871743606359\, x^{18} - 240286948785\, x^{17} - 2491355718306\, x^{16}$
$+ 65341075696\, x^{15} + 405458684553\, x^{14} - 13521774841\, x^{13} - 49483859945\, x^{12}$
$+ 2051360909\, x^{11} + 4324257587\, x^{10} - 216422271\, x^{9} - 252930808\, x^{8}$
$+ 14656655\, x^{7} + 8903427\, x^{6} - 556387\, x^{5} - 157001\, x^{4} + 9061\, x^{3} + 1014\, x^{2} - 39\, x$
$- 1$

$289, x^{136} - 136\, x^{134} + 9044\, x^{132} - 391952\, x^{130} + 12448930\, x^{128} - 308961536\, x^{126}$
$+ 6238646400\, x^{124} - 105373017600\, x^{122} + 1519059068175\, x^{120} - x^{119}$
$- 18978270773000\, x^{118} + 119\, x^{117} + 207947624041300\, x^{116} - 6902\, x^{115}$
$- 2017470039789776\, x^{114} + 260015\, x^{113} + 17465758771889714\, x^{112}$
$- 7153804\, x^{111} - 135793816793078752\, x^{110} + 153242012\, x^{109}$
$+ 953259873155160560\, x^{108} - 2660715288\, x^{107} - 6069350465113518144\, x^{106}$
$+ 38492133669\, x^{105} + 35183265977454925491\, x^{104} - 473349211335\, x^{103}$
$- 186299132550913080503\, x^{102} + 5023239206349\, x^{101}$
$+ 903603419745530393190\, x^{100} - 46545610994610\, x^{99}$
$- 4024144784291835754551\, x^{98} + 380122489789315\, x^{97}$
$+ 16488586344602668256828\, x^{96} - 2756776187630920\, x^{95}$
$- 62267456506325601199320\, x^{94} + 17865030011280200\, x^{93}$
$+ 217042306530421957172976\, x^{92} - 103981766514634960\, x^{91}$
$- 699145129000650493582057\, x^{90} + 545904274201833540\, x^{89}$
$+ 2083390060749697340814888\, x^{88} - 2594370312832985610\, x^{87}$
$- 5747904254089887742618623\, x^{86} + 11194393702777623029\, x^{85}$
$+ 14691321712375855000704434\, x^{84} - 43964780548862611815\, x^{83}$
$- 34803905871107131608802393\, x^{82} + 157486471797662594721\, x^{81}$
$+ 76444293252574820144592102\, x^{80} - 515410271337804775056\, x^{79}$
$- 155697045876778887921879636\, x^{78} + 1543225506308819240284\, x^{77}$
$+ 294061779098325213927722232\, x^{76} - 4231937986372617574235\, x^{75}$
$- 514946894268931415465896110\, x^{74} + 10637344123354850064800\, x^{73}$
$+ 835860313334836620617633835\, x^{72} - 24521877505415833228815\, x^{71}$
$- 1257110303482125776643697935\, x^{70} + 51861162213564431208618\, x^{69}$
$+ 1750819713103632174254506711\, x^{68} - 100633818488737807943617\, x^{67}$
$- 2256502011474987245904939743\, x^{66} + 179147643057797734024342\, x^{65}$
$+ 2688998228575766677067430998\, x^{64} - 292485947846198345455760\, x^{63}$
$- 2959880109744376314046472208\, x^{62} + 437720349521122420106592\, x^{61}$
$+ 3005979199869821376570696623\, x^{60} - 600021153221780736224296\, x^{59}$
$- 2812890906071473608199122712\, x^{58} + 752665830581092429983104\, x^{57}$
$+ 2421723231339482644519915528\, x^{56} - 862970305206795224207810\, x^{55}$
$- 1914995466844903887593512308\, x^{54} + 903108457497320015685570\, x^{53}$
$+ 1388226118321633567996598355\, x^{52} - 861234221148571941345793\, x^{51}$
$- 920623968098533582422981432\, x^{50} + 746988858274652420080341\, x^{49}$
$+ 557195705751922095121720282\, x^{48} - 587991216874857082812384\, x^{47}$
$- 306967756380198579519561456\, x^{46} + 418997016025807240051697\, x^{45}$

$+ 15348374833666957270651827O\ x^{44} - 26953021347000199833602O\ x^{43}$
$- 694216545448631038784631 52\ x^{42} + 156016487874481306210964\ x^{41}$
$+ 2830107024475769438524573 4\ x^{40} - 809705374187628095019 78\ x^{39}$
$- 1035641872130426286473282 6\ x^{38} + 375228870667398006215 87\ x^{37}$
$+ 338627123110906695368285 1\ x^{36} - 154546561665505650997 14\ x^{35}$
$- 984225008191780661491877\ x^{34} + 562758320276276852101 0\ x^{33}$
$+ 252806581562028819191316\ x^{32} - 180080640898379819704 0\ x^{31}$
$- 570054288030090140456 65\ x^{30} + 502916242208060735148\ x^{29}$
$+ 111988445911534240039 48\ x^{28} - 121604690822638737392\ x^{27}$
$- 189997464812097555344 8\ x^{26} + 252240613057872388 32\ x^{25}$
$+ 275551442438204644760\ x^{24} - 44399861567606851 00\ x^{23}$
$- 337531005459169319 15\ x^{22} + 654737234933334245\ x^{21}$
$+ 344227344231263562 0\ x^{20} - 79644411056281331\ x^{19}$
$- 287230018776403296\ x^{18} + 7841900319426338\ x^{17} + 19190704429715212\ x^{16}$
$- 610323342074791\ x^{15} - 998882253604430\ x^{14} + 36414986108936\ x^{13}$
$+ 39073463666536\ x^{12} - 1598791743652\ x^{11} - 1093788648512\ x^{10}$
$+ 48768230072\ x^{9} + 20437291897\ x^{8} - 948906221\ x^{7} - 229757023\ x^{6}$
$+ 10290678\ x^{5} + 1322175\ x^{4} - 49946\ x^{3} - 2890\ x^{2} + 68\ x + 1$

$361, x^{171} - 171\ x^{169} + 14364\ x^{167} - 790077\ x^{165} + 32005215\ x^{163} - 1018228563\ x^{161}$
$+ 26494512912\ x^{159} - 579786718968\ x^{157} + 10889675092764\ x^{155}$
$- 178282952307460\ x^{153} - x^{152} + 2575247415442416\ x^{151} + 152\ x^{150}$
$- 33141678386233365\ x^{149} - 11324\ x^{148} + 383039985206089185\ x^{147}$
$+ 551152\ x^{146} - 4002338930132953305\ x^{145} - 19709270\ x^{144}$
$+ 38020398935930875800\ x^{143} + 552181344\ x^{142} - 329932572988466822220\ x^{141}$
$- 12620747568\ x^{140} + 2626156851125941560735\ x^{139} + 241970194752\ x^{138}$
$- 19241764980251264712765\ x^{137} - 3971083769081\ x^{136}$
$+ 130178854434292506945620\ x^{135} + 56650425796680\ x^{134}$
$- 815420871439179865182224\ x^{133} - 711002738414388\ x^{132}$
$+ 4740241330790146262628722\ x^{131} + 7926924147428496\ x^{130}$
$- 25627399956621012969061006\ x^{129} - 79127689257366594\ x^{128}$
$+ 129090795632619330733397888\ x^{127} + 711842676573188352\ x^{126}$
$- 606848093922789227486208000\ x^{125} - 5803065298150992000\ x^{124}$
$+ 2666141002211800744116300975\ x^{123} + 43069757628904588800\ x^{122}$
$- 10961126542243912863171158805\ x^{121} - 292185552443883060600\ x^{120}$

$$+ 422163282210561311713159743 80\ x^{119} + 1818043437428605710400\ x^{118}$$
$$- 1524695681275900695199158 30771\ x^{117} - 1040626355602791477520 0\ x^{116}$$
$$+ 5168124322246884064862963 17877\ x^{115} + 5493452941725856078399 9\ x^{114}$$
$$- 1645315926776509116211487153969\ x^{113} - 2680555333155775681890 86\ x^{112}$$
$$+ 4922723018743143015771064620232\ x^{111}$$
$$+ 12113654635329917585280 73\ x^{110}$$
$$- 13849411995127589647624030519820\ x^{109}$$
$$- 50784167509652346797817 90\ x^{108}$$
$$+ 36653614659766570363771369178682\ x^{107}$$
$$+ 197796373354075672209096 81\ x^{106}$$
$$- 91287944108711140193002679400774\ x^{105}$$
$$- 716625532366817131705590 09\ x^{104}$$
$$+ 214011238657602807138198846567384\ x^{103}$$
$$+ 2417792977232549626390031 26\ x^{102}$$
$$- 472353376751409455238089154417837\ x^{101}$$
$$- 7603206120711149434988419 68\ x^{100}$$
$$+ 981639733577962352020455196369525\ x^{99}$$
$$+ 22302737954086035914164637 71\ x^{98}$$
$$- 1920909377807947631865605229331485\ x^{97}$$
$$- 61062738188808114905978804 28\ x^{96}$$
$$+ 3539277428995011521576828975856721\ x^{95}$$
$$+ 156123401256498257625518413 40\ x^{94}$$
$$- 6139422579817114290751462232825255\ x^{93}$$
$$- 372904583001175461666439234 96\ x^{92}$$
$$+ 10024599158934579725109861627735500\ x^{91}$$
$$+ 832299965045535273023977032 52\ x^{90}$$
$$- 15403652366106083870950841054955225\ x^{89}$$
$$- 1736125708337110615946136242 73\ x^{88}$$
$$+ 22266778392455713827692696569295790\ x^{87}$$
$$+ 3384715666673706632818018658 40\ x^{86}$$
$$- 30268901876715602143375286298244849\ x^{85}$$
$$- 6167066680802225677922798890 36\ x^{84}$$
$$+ 38675726448112291203090102550029591\ x^{83}$$
$$+ 10499826348846216315325596774 86\ x^{82}$$
$$- 46424513965964683124084181827316398\ x^{81}$$
$$- 16700154839301806773566171007 86\ x^{80}$$

$$+ 52318408775097656106233348982527274 \quad x^{79}$$
$$+ 2480493033700986394606152596391 \quad x^{78}$$
$$- 55316752708095845185073814465219402 \quad x^{77}$$
$$- 3439021505141170575801201741715 \quad x^{76}$$
$$+ 54829545507176871188653105133284977 \quad x^{75}$$
$$+ 4448019645765961766094236265391 \quad x^{74}$$
$$- 50903977459581248214051956417695665 \quad x^{73}$$
$$- 5363437974393389092408205061779 \quad x^{72}$$
$$+ 44223356199974624133412436384368176 \quad x^{71}$$
$$+ 6024586886883371442158683856322 \quad x^{70}$$
$$- 35913411685908932547191745736620936 \quad x^{69}$$
$$- 6298431743933124286369407104705 \quad x^{68}$$
$$+ 27231048238261039371617775220490642 \quad x^{67}$$
$$+ 6122392790970479616905840998639 \quad x^{66}$$
$$- 19254188331076281628456950101799653 \quad x^{65}$$
$$- 5527160152801882996991491193110 \quad x^{64}$$
$$+ 12677654582740504674451656065493412 \quad x^{63}$$
$$+ 4628350921755874319120288231640 \quad x^{62}$$
$$- 7761585702639791900149222241771004 \quad x^{61}$$
$$- 3589914501446225977928720321160 \quad x^{60}$$
$$+ 4411087203879034519087304023191142 \quad x^{59}$$
$$+ 2575136215173141239218779295240 \quad x^{58}$$
$$- 2322982216258236833733170019830053 \quad x^{57}$$
$$- 1705408688999865652850569469116 \quad x^{56}$$
$$+ 1131363673884221727073486814958743 \quad x^{55}$$
$$+ 1040748677728253183412451655888 \quad x^{54}$$
$$- 508497085604729741695713188899623 \quad x^{53}$$
$$- 584043629251708172386162801143 \quad x^{52}$$
$$+ 210422968035394028065142003782640 \quad x^{51}$$
$$+ 300695689399679026014938225178 \quad x^{50}$$
$$- 79966900262188517241468259511205 \quad x^{49}$$
$$- 141673893800146688633660824922 \quad x^{48}$$
$$+ 27830977153284476469496104763500 \quad x^{47}$$
$$+ 60914073903721716100274226606 \quad x^{46}$$
$$- 8843378682765458854884063243412 \quad x^{45}$$
$$- 23826911227443554886147436365 \quad x^{44}$$

$$
\begin{aligned}
&+ 2556918482472241740466862021739 \; x^{43} \\
&+ 8449941147086039130459520922 \; x^{42} \\
&- 670209611880148460328103032887 \; x^{41} \\
&- 2706612776749232859453041004 \; x^{40} \\
&+ 158603643859477135744645251485 \; x^{39} \\
&+ 779739576224176104957780515 \; x^{38} - 33731795307512615631685361584 \; x^{37} \\
&- 201082407483829499074657097 \; x^{36} + 6414668798903932039019444661 \; x^{35} \\
&+ 46174318854602291385153877 \; x^{34} - 1084507602604250052653589395 \; x^{33} \\
&- 9385069153011300788028996 \; x^{32} + 161961167641722148758645755 \; x^{31} \\
&+ 1677054800099593553802080 \; x^{30} - 21209203125554867682371853 \; x^{29} \\
&- 261442713266780528651036 \; x^{28} + 2415052200855693336092278 \; x^{27} \\
&+ 35242502172426819807057 \; x^{26} - 236811893435427144846167 \; x^{25} \\
&- 4065696219861766884111 \; x^{24} + 19771155592363831106420 \; x^{23} \\
&+ 396563381677436155039 \; x^{22} - 1386707683675987601461 \; x^{21} \\
&- 32234526397458505072 \; x^{20} + 80400226409694878562 \; x^{19} \\
&+ 2145611516419256525 \; x^{18} - 3778080549289386619 \; x^{17} \\
&- 114441894364371884 \; x^{16} + 140374143225524486 \; x^{15} + 4758488994631147 \; x^{14} \\
&- 3994837216213399 \; x^{13} - 148780653430967 \; x^{12} + 83483349338804 \; x^{11} \\
&+ 3330574085917 \; x^{10} - 1209027170924 \; x^{9} - 49785640321 \; x^{8} + 11170600517 \; x^{7} \\
&+ 447898837 \; x^{6} - 58177449 \; x^{5} - 2063115 \; x^{4} + 138605 \; x^{3} + 3610 \; x^{2} - 95 \; x - 1
\end{aligned}
$$

3.3.4. $q = 2^k$ için $P^*_{2^k}$ minimal polinomları

$k \in \mathbb{N}, k \geq 2$ ve $q = 2^k > 3$ olsun. Sonuç 2.6.1'den $q = 2^k$ çift olmak üzere $\lambda_{2^k} = 2cos(\pi/2^k)$'nın $P^*_{2^k}$ minimal polinomunun hesabı için elde edilen $k \in \mathbb{N}$ olmak üzere

$$P^*_{2^k}(x) = \frac{D_{2^k+1}(x) - D_{2^k-1}(x)}{D_{2^{k-1}+1}(x) - D_{2^{k-1}-1}(x)}$$

kuralı Maple'da bir döngü içinde ifade edilmelidir. Bu kural sadece Dickson polinomlarına bağlı olup bir önceki minimal polinomlara göre hesaplanması daha kolaydır. Yine bir önceki polinomların hesaplanmasına benzer şekilde (2.2)'deki tanım kullanılarak bu döngü içindeki Dickson polinomları MAPLE'a anlatılmalıdır. $P^*_{2^k}$ minimal polinomunun hesabı için yapılan tüm bu hazırlıklardan sonra MAPLE artık ikinin kuvvetleri şeklindeki minimal polinomların genişleyen bir listesini vermeye hazırdır.

Aşağıda $q = 2^k$ olmak üzere $P^*_{2^k}$ minimal polinomunun hesabı için oluşturulan algoritma ve bu algoritma içindeki döngüye ait genişleyen bir liste görülmektedir. Bu döngüde $k \in \mathbb{N}$ değerleri $2 \leq k \leq 8$ için sınırlandırılmıştır. Bu döngü ile artan k değerleri için istenildiği kadar uzun bir liste elde edilebilir.

```
> f:=proc(x)local k;for k from 2 to 8 do
print(2^k,evala(Divide(sort((sort(sum((-1)^i*(2^k+1)*(2^k-
i)!/(2^k+1-2*i)!*1/i!*x^(2^k+1-2*i),i=0..2^(k-1))))-
(sort(sum((-1)^i*(2^k-1)*(2^k-2-i)!/(2^k-1-
2*i)!*1/i!*x^(2^k-1-2*i),i=0..2^(k-1)-
1)))),sort((sort(sum((-1)^i*(2^(k-1)+1)*(2^(k-1)-i)!/(2^(k-
1)+1-2*i)!*1/i!*x^(2^(k-1)+1-2*i),i=0..2^(k-2))))-
(sort(sum((-1)^i*(2^(k-1)-1)*(2^(k-1)-2-i)!/(2^(k-1)-1-
2*i)!*1/i!*x^(2^(k-1)-1-2*i),i=0..2^(k-2)-
1)))),'q')),sort(q));end do;end proc;
```

```
f := proc(x)
local k;
    for k from 2 to 8 do print(2^k, evala(Divide(sort(sort(sum(
        (-1)^i×(2^k + 1)×(2^k − i)!×x^(2^k + 1 − 2×i)/((2^k + 1 − 2×i)!×i!),
        i = 0 .. 2^(k − 1))) − sort(sum(
        (-1)^i×(2^k − 1)×(2^k − 2 − i)!×x^(2^k − 1 − 2×i)/((2^k − 1 − 2×i)!×i!),
        i = 0 .. 2^(k − 1) − 1))), sort(sort(sum((-1)^i×(2^(k − 1) + 1)×
        (2^(k − 1) − i)!×x^(2^(k − 1) + 1 − 2×i)/((2^(k − 1) + 1 − 2×i)!×i!),
        i = 0 .. 2^(k − 2))) − sort(sum((-1)^i×(2^(k − 1) − 1)×
        (2^(k − 1) − 2 − i)!×x^(2^(k − 1) − 1 − 2×i)/((2^(k − 1) − 1 − 2×i)!×i!),
        i = 0 .. 2^(k − 2) − 1))), 'q')), sort(q))
    end do
end proc
```

```
> f(x);
```

$$4,\ true,\ x^2 - 2$$

$$8,\ true,\ x^4 - 4x^2 + 2$$

$$16,\ true,\ x^8 - 8x^6 + 20x^4 - 16x^2 + 2$$

$$32,\ true,\ x^{16} - 16x^{14} + 104x^{12} - 352x^{10} + 660x^8 - 672x^6 + 336x^4 - 64x^2 + 2$$

$$64,\ true,\ x^{32} - 32x^{30} + 464x^{28} - 4032x^{26} + 23400x^{24} - 95680x^{22} + 283360x^{20} - 615296x^{18} + 980628x^{16} - 1136960x^{14} + 940576x^{12} - 537472x^{10} + 201552x^8 - 45696x^6 + 5440x^4 - 256x^2 + 2$$

$128, \mathit{true}, x^{64} - 64\, x^{62} + 1952\, x^{60} - 37760\, x^{58} + 520144\, x^{56} - 5430656\, x^{54}$
$+ 44662464\, x^{52} - 296854272\, x^{50} + 1623421800\, x^{48} - 7398867840\, x^{46}$
$+ 28362326720\, x^{44} - 92043777280\, x^{42} + 254005423840\, x^{40} - 597659820800\, x^{38}$
$+ 1200442440064\, x^{36} - 2057901325824\, x^{34} + 3006465218196\, x^{32}$
$- 3732682723968\, x^{30} + 3922021702720\, x^{28} - 3467892873984\, x^{26}$
$+ 2561511781920\, x^{24} - 1565841089280\, x^{22} + 782920544640\, x^{20}$
$- 315492902400\, x^{18} + 100563362640\, x^{16} - 24754058496\, x^{14} + 4559958144\, x^{12}$
$- 602516992\, x^{10} + 53796160\, x^{8} - 2968064\, x^{6} + 87296\, x^{4} - 1024\, x^{2} + 2$

$256, \mathit{true}, x^{128} - 128\, x^{126} + 8000\, x^{124} - 325376\, x^{122} + 9683872\, x^{120} - 224854784\, x^{118}$
$+ 4240908672\, x^{116} - 66793059840\, x^{114} + 896279371728\, x^{112}$
$- 10403870354176\, x^{110} + 105713903005568\, x^{108} - 949207352861184\, x^{106}$
$+ 7589567411885760\, x^{104} - 54380900412120576\, x^{102}$
$+ 351022578975981312\, x^{100} - 2050220372780067840\, x^{98}$
$+ 10875778383731766120\, x^{96} - 52563380423759251200\, x^{94}$
$+ 232075288719446148480\, x^{92} - 938162393606568399360\, x^{90}$
$+ 3479018876291024480960\, x^{88} - 11853746558470887150080\, x^{86}$
$+ 37157327333800250886400\, x^{84} - 107271588476710289515520\, x^{82}$
$+ 285455885682015121379040\, x^{80} - 700614057285567210530304\, x^{78}$
$+ 1586684776793784565024512\, x^{76} - 3316502833782387979699200\, x^{74}$
$+ 6398481538604449952262528\, x^{72} - 11392907567170305871113216\, x^{70}$
$+ 18716919574636931073971712\, x^{68} - 28358591813118010632861696\, x^{66}$
$+ 39602330364022221879875220\, x^{64} - 50933523453823795412968704\, x^{62}$
$+ 60272398530150686561904768\, x^{60} - 65549705313896599210182144\, x^{58}$
$+ 65430955847748235805815872\, x^{56} - 59853681024967201152929280\, x^{54}$
$+ 50088080436683078859556608\, x^{52} - 38269544603308419802807296\, x^{50}$
$+ 26636472806280008101385760\, x^{48} - 16846616947285589648647680\, x^{46}$
$+ 9654622669125462506284800\, x^{44} - 4997687028723768826782720\, x^{42}$
$+ 2328467820200846839751040\, x^{40} - 972532744180273378851840\, x^{38}$
$+ 362508228610144318840320\, x^{36} - 119979082755130507417600\, x^{34}$
$+ 35056388242514695136080\, x^{32} - 8983708896040965532160\, x^{30}$
$+ 2004058138347600003328\, x^{28} - 385807983853013904384\, x^{26}$
$+ 63455260502140444800\, x^{24} - 8811900326334974976\, x^{22}$
$+ 1018793280972662272\, x^{20} - 96423772545357824\, x^{18} + 7317875594960192\, x^{16}$
$- 433973348848640\, x^{14} + 19453977707008\, x^{12} - 630784833536\, x^{10}$
$+ 13914371328\, x^{8} - 190654464\, x^{6} + 1397760\, x^{4} - 4096\, x^{2} + 2$

3.3.5 $q = 2^2 p$ için $P^*_{2^2 p}$ minimal polinomları

$q \in \mathbb{N}$, $q = 2^2 p \geq 3$ ve $p > 2$ asal olsun. Teorem 2.5.5'ten $q = 2^2 p$ çift olmak üzere $\lambda_{2^2 p} = 2cos(\pi/2^2 p)$'nin $P^*_{2^2 p}$'nin minimal polinomunun hesabı için (2.6) eşitliği kullanılırsa

$$q = 2^2 3 = 12 \text{ için} \qquad P^*_{12}(x) = 2^{\frac{\varphi(24)-12}{2}} . \frac{D_{13}(x) - D_{11}(x)}{\prod_{\substack{d|24 \\ d \neq 24 \\ d \nmid 12}} \psi_d\left(\frac{x}{2}\right) . [D_7(x) - D_5(x)]} \tag{3.63}$$

eşitliği alınır. (3.63)'te φ Euler fonksiyonu olmak üzere $\varphi(24) = \varphi(2^3)\varphi(3) = 2^2 2$ =eşitliği geçerli olur. (3.63)'te çarpım sembolü altındaki koşullar incelendiğinde $d|24$'ün d bölenleri: 1, 2, 3, 4, 6, 8, 12, 24'tür. Bu d bölenlerinin $d \neq 24$ ve $d \nmid 12$ koşulları için d böleni sadece 8'dir. O halde çarpım sembolü için

$$\prod_{\substack{d|24 \\ d \neq 24 \\ d \nmid 12}} \psi_d(x/2) = \psi_8(x/2) \tag{3.64}$$

eşitliği elde edilir. (3.64), (3.63)'te ele alnırsa minimal polinom,

$$q = 2^2 3 = 12 \text{ için} \qquad P^*_{12}(x) = 2^{\frac{\varphi(24)-12}{2}} . \frac{D_{13}(x) - D_{11}(x)}{\psi_8\left(\frac{x}{2}\right) . [D_7(x) - D_5(x)]}$$

şeklinde bulunur. Benzer şekilde

$$q = 2^2 5 = 20 \text{ için} \qquad P^*_{20}(x) = 2^{-2} . \frac{D_{13}(x) - D_{11}(x)}{\prod_{\substack{d|24 \\ d \neq 24 \\ d \nmid 12}} \psi_d\left(\frac{x}{2}\right) . [D_7(x) - D_5(x)]} \tag{3.65}$$

eşitliği alınır. (3.65)'te φ Euler fonksiyonu olmak üzere $\varphi(40) = \varphi(2^3)\varphi(5) = 2^2 4$ =16 eşitliği geçerli olur. (3.65)'te çarpım sembolü altındaki koşullar incelendiğinde $d|40$'ün d bölenleri: 1, 2, 4, 5, 8, 10, 20, 40'tır. Bu d bölenlerinin $d \neq 40$ ve $d \nmid 20$ koşulları için d böleni sadece 8'dir. O halde çarpım sembolü için

$$\prod_{\substack{d|40 \\ d\neq 40 \\ d\nmid 20}} \psi_d(x/2) = \psi_8(x/2) \tag{3.66}$$

eşitliği elde edilir. (3.66), (3.65)’te ele alınırsa minimal polinom,

$q = 2^2 5 = 20$ için $$P_{20}^*(x) = 2^{-2}.\frac{D_{21}(x)-D_{19}(x)}{\psi_8\left(\frac{x}{2}\right).[D_{11}(x)-D_9(x)]} \tag{3.67}$$

biçiminde elde edilir. (3.67)’de $\psi_8(x) = x^2 - 1/2$ olmak üzere $\psi_8(x/2) = (x^2 - 2)/4$ eşitliği düşünülürse istenilen minimal polinom

$q = 2^2 5 = 20$ için $$P_{20}^*(x) = 2^{-2}.\frac{D_{21}(x)-D_{19}(x)}{2^{-2}(x^2-2).[D_{11}(x)-D_9(x)]}$$

şeklinde alınır. Bu şekilde yapılmaya devam edildiğinde

$q = 2^2 7 = 28$ için $$P_{28}^*(x) = \frac{D_{29}(x)-D_{27}(x)}{(x^2-2).[D_{15}(x)-D_{13}(x)]}$$

$q = 2^2 11 = 44$ için $$P_{44}^*(x) = \frac{D_{45}(x)-D_{43}(x)}{(x^2-2).[D_{23}(x)-D_{21}(x)]}$$

$q = 2^2 13 = 46$ için $$P_{28}^*(x) = \frac{D_{47}(x)-D_{45}(x)}{(x^2-2).[D_{24}(x)-D_{22}(x)]}$$

$\vdots$ $\vdots$

belli kuralı takip eden eşitlikler bulunur. Bu eşitliklerdeki kuralı aşağıdaki teormde veriyoruz.

Teorem 3.3.5.1. $q = 2^2 p \geq 3$ ve $p > 2$ asal sayı olsun. O zaman $k \in \mathbb{N}$, $p = 2k + 1$ olmak üzere P_{4p}^* minimal polinomu,

$$P_{4p}^* = P_{8k+4}^*(x) = \frac{D_{8k+5}(x)-D_{8k+3}(x)}{(x^2-2)[D_{4k+3}(x)-D_{4k+1}(x)]} \tag{3.68}$$

şeklindedir.

İspat. $q \in \mathbb{N}$, $q = 2^2 p > 3$ ve $p > 2$ asal sayı olsun. Teorem 2.5.5'ten $q = 2^2 p$ çift olmak üzere $P^*_{2^2 p}$Minimal polinomunun hesabı için (2.6) eşitliği kullanılırsa

$$q = 2^2 p \text{ için} \qquad P^*_{4p}(x) = 2^{\frac{\varphi(8p)-4p}{2}} . \frac{D_{4p+1}(x) - D_{4p-1}(x)}{\prod_{\substack{d|8p \\ d\neq 8p \\ d\nmid 4p}} \psi_d\left(\frac{x}{2}\right) . \left[D_{2p+1}(x) - D_{2p-1}(x)\right]} \tag{3.69}$$

eşitliği alınır. (3.69)'da φ Euler fonksiyonu olmak üzere

$$\varphi(8p) = \varphi(2^3)\varphi(p) = 2^2(p-1) = 4p - 4 \tag{3.70}$$

eşitliği geçerli olur. (3.69)'da çarpım sembolü altındaki koşullar incelendiğinde $d|8p$'nin d bölenleri: 1, 2, 4, 8, p, 2p, 4p, 8p'dir. Bu d bölenlerinin $d \neq 8p$ ve $d \nmid 4p$ koşulları için d böleni sadece 8'dir. O halde çarpım sembolü için

$$\prod_{\substack{d|8p \\ d\neq 8p \\ d\nmid 4p}} \psi_d(x/2) = \psi_8(x/2) \tag{3.71}$$

eşitliği elde edilir. (3.71)'de $\psi_8(x) = x^2 - 1/2$ olmak üzere

$$\prod_{\substack{d|8p \\ d\neq 8p \\ d\nmid 4p}} \psi_d(x/2) = \psi_8(x/2) = x^2/4 - 1/2 = (x^2 - 2)/4 \tag{3.72}$$

eşitliği bulunur. (3.72) ve (3.70) eşitlikleri (3.69)'da ele alınırsa minimal polinom

$$q = 2^2 p \text{ için} \qquad P^*_{4p}(x) = 2^{\frac{4p-4-4p}{2}} . \frac{D_{4p+1}(x) - D_{4p-1}(x)}{2^{-2}(x^2-2)\left[D_{2p+1}(x) - D_{2p-1}(x)\right]}$$

$$q = 2^2 p \text{ için} \qquad P^*_{4p}(x) = \frac{D_{4p+1}(x) - D_{4p-1}(x)}{(x^2-2)\left[D_{2p+1}(x) - D_{2p-1}(x)\right]} \tag{3.73}$$

biçiminde bulunur. Son olarak (3.73)'teki kural $k \in \mathbb{N}$, $p = 2k + 1$ olmak üzere

$$P_{4p}^{*}(x) = P_{8k+4}^{*}(x) = \frac{D_{8k+5}(x) - D_{8k+3}(x)}{(x^2-2)[D_{4k+3}(x) - D_{4k+1}(x)]}$$

şeklindedir.

Aşağıdaki $k \in \mathbb{N}$, $p = 2k + 1$ olmak üzere P_{4p}^{*} minimal polinomunun hesabı için yapılan algoritma teorem 3.3.5.1'in uygulamasıdır.

$k \in \mathbb{N}$, $p = 2k + 1$ olmak üzere P_{4p}^{*} minimal polinomunun hesabı için (3.68) kuralı MAPLE'da bir döngü içinde ifade edilmelidir. Böylece bu döngü ile $k \in \mathbb{N}$ için istenen minimal polinomların bir listesi kolaylıkla çok kısa bir zaman diliminde elde edilir. (3.68) kuralı, Dickson polinomlarına bağlı olup (2.2)'deki tanım kullanılarak Dickson polinomları MAPLE'da bu döngü içinde anlatılmalıdır. Böylece yapılan tüm bu hazırlıklardan sonra istenen minimal polinomların hesabı için MAPLE hazır olarak beklemektedir.

Aşağıda $q = 2^2 p$ olmak üzere P_{4p}^{*} minimal polinomununun hesabına ilişkin bir algoritma ve bu algoritmaya ait bir liste görülmektedir. Bu algoritmadaki döngü, $k \in \mathbb{N}$ olmak üzere $1 \leq k \leq 25$ için sınırlandırılmıştır. k değerleri artıkça bu listede uzayacaktır.

```
> f:=proc(x)local k,A,B,E,F,PAY,PAYDA,MINPOL;for k from 1
to 25 do if isprime(2*k+1) then A:=sort(sum((-
1)^i*(8*k+5)*(8*k+4-i)!/(8*k+5-2*i)!*1/i!*x^(8*k+5-
2*i),i=0..(4*k+2)));B:=sort(sum((-1)^i*(8*k+3)*(8*k+2-
i)!/(8*k+3-2*i)!*1/i!*x^(8*k+3-
2*i),i=0..(4*k+1)));E:=sort(sum((-1)^i*(4*k+3)*(4*k+2-
i)!/(4*k+3-2*i)!*1/i!*x^(4*k+3-
2*i),i=0..(2*k+1)));F:=sort(sum((-1)^i*(4*k+1)*(4*k-
i)!/(4*k+1-2*i)!*1/i!*x^(4*k+1-2*i),i=0..2*k));PAY:=sort(A-
B);PAYDA:=sort(expand((x^2-2)*(E-
F)));evala(Divide(PAY,PAYDA,'q'));MINPOL:=sort(q);print(4*(
2*k+1),MINPOL);end if;end do;end proc;
```

```
f := proc(x)
local k, A, B, E, F, PAY, PAYDA, MINPOL;
    for k to 25 do
        if isprime(2×k + 1) then
            A := sort(sum((-1)^i×(8×k + 5)×(8×k + 4 − i)!×x^(8×k + 5 − 2×i)/(
                (8×k + 5 − 2×i)!×i!), i = 0 .. 4×k + 2));
            B := sort(sum((-1)^i×(8×k + 3)×(8×k + 2 − i)!×x^(8×k + 3 − 2×i)/(
                (8×k + 3 − 2×i)!×i!), i = 0 .. 4×k + 1));
            E := sort(sum((-1)^i×(4×k + 3)×(4×k + 2 − i)!×x^(4×k + 3 − 2×i)/(
                (4×k + 3 − 2×i)!×i!), i = 0 .. 2×k + 1));
            F := sort(sum((-1)^i×(4×k + 1)×(4×k − i)!×x^(4×k + 1 − 2×i)/(
                (4×k + 1 − 2×i)!×i!), i = 0 .. 2×k));
            PAY := sort(A − B);
            PAYDA := sort(expand((x^2 − 2)×(E − F)));
            evala(Divide(PAY, PAYDA, 'q'));
            MINPOL := sort(q);
            print(8×k + 4, MINPOL)
        end if
    end do
end proc
```

```
> f(x);
```

$$12, x^4 - 4x^2 + 1$$

$$20, x^8 - 8x^6 + 19x^4 - 12x^2 + 1$$

$$28, x^{12} - 12x^{10} + 53x^8 - 104x^6 + 86x^4 - 24x^2 + 1$$

$$44, x^{20} - 20x^{18} + 169x^{16} - 784x^{14} + 2172x^{12} - 3664x^{10} + 3683x^8 - 2072x^6 + 575x^4 - 60x^2 + 1$$

$$52, x^{24} - 24x^{22} + 251x^{20} - 1500x^{18} + 5645x^{16} - 13904x^{14} + 22580x^{12} - 23792x^{10} + 15622x^8 - 5936x^6 + 1141x^4 - 84x^2 + 1$$

$$68, x^{32} - 32x^{30} + 463x^{28} - 4004x^{26} + 23051x^{24} - 93128x^{22} + 271214x^{20} - 575832x^{18} + 891311x^{16} - 995824x^{14} + 786798x^{12} - 425128x^{10} + 149106x^8 - 31248x^6 + 3396x^4 - 144x^2 + 1$$

$$76, x^{36} - 36x^{34} + 593x^{32} - 5920x^{30} + 39992x^{28} - 193312x^{26} + 689479x^{24} - 1844392x^{22} + 3724921x^{20} - 5673268x^{18} + 6463399x^{16} - 5422832x^{14} + 3269436x^{12} - 1365584x^{10} + 374154x^8 - 61776x^6 + 5325x^4 - 180x^2 + 1$$

$92, x^{44} - 44\,x^{42} + 901\,x^{40} - 11400\,x^{38} + 99790\,x^{36} - 641208\,x^{34} + 3131721\,x^{32}$
$- 11878176\,x^{30} + 35442612\,x^{28} - 83778736\,x^{26} + 157236844\,x^{24} - 233880352\,x^{22}$
$+ 274130056\,x^{20} - 250699168\,x^{18} + 176290339\,x^{16} - 93382192\,x^{14}$
$+ 36217051\,x^{12} - 9883588\,x^{10} + 1792219\,x^{8} - 197912\,x^{6} + 11506\,x^{4} - 264\,x^{2} + 1$

$116, x^{56} - 56\,x^{54} + 1483\,x^{52} - 24700\,x^{50} + 290277\,x^{48} - 2559856\,x^{46} + 17587868\,x^{44}$
$- 96490064\,x^{42} + 429799106\,x^{40} - 1572206416\,x^{38} + 4758952209\,x^{36}$
$- 11975579620\,x^{34} + 25110054325\,x^{32} - 43876783008\,x^{30} + 63779090680\,x^{28}$
$- 76834704416\,x^{26} + 76272587666\,x^{24} - 61891406768\,x^{22} + 40618566074\,x^{20}$
$- 21264132872\,x^{18} + 8722366766\,x^{16} - 2738913248\,x^{14} + 638430104\,x^{12}$
$- 105945632\,x^{10} + 11797916\,x^{8} - 806624\,x^{6} + 29225\,x^{4} - 420\,x^{2} + 1$

$124, x^{60} - 60\,x^{58} + 1709\,x^{56} - 30744\,x^{54} + 392042\,x^{52} - 3770312\,x^{50} + 28406573\,x^{48}$
$- 171941744\,x^{46} + 850725382\,x^{44} - 3482700936\,x^{42} + 11896934698\,x^{40}$
$- 34104425744\,x^{38} + 82326715876\,x^{36} - 167611886480\,x^{34} + 287773698725\,x^{32}$
$- 415946451104\,x^{30} + 504468371930\,x^{28} - 510846665944\,x^{26}$
$+ 429009013834\,x^{24} - 296151525232\,x^{22} + 166151227156\,x^{20} - 74673011728\,x^{18}$
$+ 26393382334\,x^{16} - 7164470752\,x^{14} + 1447699396\,x^{12} - 208761904\,x^{10}$
$+ 20242444\,x^{8} - 1207136\,x^{6} + 38200\,x^{4} - 480\,x^{2} + 1$

$148, x^{72} - 72\,x^{70} + 2483\,x^{68} - 54604\,x^{66} + 860081\,x^{64} - 10332736\,x^{62} + 98445520\,x^{60}$
$- 763615936\,x^{58} + 4912530808\,x^{56} - 26567853632\,x^{54} + 122005197367\,x^{52}$
$- 479298795820\,x^{50} + 1619649684367\,x^{48} - 4726281748816\,x^{46}$
$+ 11940711503788\,x^{44} - 26157084622864\,x^{42} + 49703995018057\,x^{40}$
$- 81887447386216\,x^{38} + 116801377428793\,x^{36} - 143899865922244\,x^{34}$
$+ 152619992398647\,x^{32} - 138741084924896\,x^{30} + 107508408091128\,x^{28}$
$- 70526067712544\,x^{26} + 38839881428636\,x^{24} - 17773144044704\,x^{22}$
$+ 6673266886466\,x^{20} - 2024178913320\,x^{18} + 486479767130\,x^{16}$
$- 90381694624\,x^{14} + 12571379640\,x^{12} - 1254035872\,x^{10} + 84470637\,x^{8}$
$- 3511656\,x^{6} + 77691\,x^{4} - 684\,x^{2} + 1$

$$164, x^{80} - 80 x^{78} + 3079 x^{76} - 75924 x^{74} + 1347727 x^{72} - 18345336 x^{70} + 199187658 x^{68} - 1771705320 x^{66} + 13157412633 x^{64} - 82736212544 x^{62} + 445213386648 x^{60} - 2066825134496 x^{58} + 8329054199560 x^{56} - 29274668605376 x^{54} + 90056706039088 x^{52} - 243081111087040 x^{50} + 576633114411292 x^{48} - 1203157820620096 x^{46} + 2208348122251723 x^{44} - 3563549361535204 x^{42} + 5049211508078887 x^{40} - 6269731720797016 x^{38} + 6804719429352538 x^{36} - 6433244351722984 x^{34} + 5275595237027707 x^{32} - 3733313512759648 x^{30} + 2265672394068988 x^{28} - 1170406386974352 x^{26} + 510062813607460 x^{24} - 185514666806880 x^{22} + 55581847347800 x^{20} - 13500673175520 x^{18} + 2606441018351 x^{16} - 390075869936 x^{14} + 43812658163 x^{12} - 3536702180 x^{10} + 193133347 x^{8} - 6519128 x^{6} + 117250 x^{4} - 840 x^{2} + 1$$

$$172, x^{84} - 84 x^{82} + 3401 x^{80} - 88400 x^{78} + 1657580 x^{76} - 23888016 x^{74} + 275261683 x^{72} - 2605081944 x^{70} + 20641525767 x^{68} - 138895391516 x^{66} + 802331567673 x^{64} - 4011973088320 x^{62} + 17478618298384 x^{60} - 66676798012864 x^{58} + 223575454091432 x^{56} - 660837298096320 x^{54} + 1725292971075116 x^{52} - 3983703211746032 x^{50} + 8140220076616508 x^{48} - 14720097887038784 x^{46} + 23542541967477872 x^{44} - 33262364508282176 x^{42} + 41442154829036603 x^{40} - 45424160999017784 x^{38} + 43668623045688857 x^{36} - 36682966847295428 x^{34} + 26804238294337451 x^{32} - 16944525904468576 x^{30} + 9207363507071672 x^{28} - 4267596836387616 x^{26} + 1671852059963700 x^{24} - 547544986395360 x^{22} + 147947936173495 x^{20} - 32453763983180 x^{18} + 5665357670215 x^{16} - 767493625840 x^{14} + 78107277156 x^{12} - 5717714992 x^{10} + 283352663 x^{8} - 8684984 x^{6} + 141911 x^{4} - 924 x^{2} + 1$$

$$188, x^{92} - 92 x^{90} + 4093 x^{88} - 117304 x^{86} + 2434146 x^{84} - 38971240 x^{82} + 500938613 x^{80} - 5311633808 x^{78} + 47372938394 x^{76} - 360581199416 x^{74} + 2368557046838 x^{72} - 13544007971504 x^{70} + 67884642590732 x^{68} - 299860288149936 x^{66} + 1172358295216073 x^{64} - 4070657552017984 x^{62} + 12585278279264452 x^{60} - 34713306066102256 x^{58} + 85536014835042788 x^{56} - 188441264893928160 x^{54} + 371293785926442536 x^{52} - 654203436349543712 x^{50} + 1030159891033766828 x^{48} - 1448246397445934144 x^{46} + 1815010360454788472 x^{44}$$

$- 2023783065506411168\ x^{42} + 2002771405129173992\ x^{40}$
$- 1753816635422424640\ x^{38} + 1354163663820738000\ x^{36}$
$- 918031553069301568\ x^{34} + 543734909327844643\ x^{32}$
$- 279725969031640160\ x^{30} + 124145955780384403\ x^{28}$
$- 47152781754674964\ x^{26} + 15182764013432175\ x^{24} - 4098110176432680\ x^{22}$
$+ 914856413523510\ x^{20} - 166170276827640\ x^{18} + 24067143465195\ x^{16}$
$- 2709888043440\ x^{14} + 229576687990\ x^{12} - 14009166600\ x^{10} + 579402890\ x^{8}$
$- 14835920\ x^{6} + 202676\ x^{4} - 1104\ x^{2} + 1$

Yukarıda $q \in \mathbb{N}$, $q \geq 3$'ün bazı değerleri için belli bir kuralı izleyen P_q^* minimal polinomlarının kolayca elde edildiği görülmüştür. Buna karşın $q \in \mathbb{N}$'nin bazı değerleri için de P_q^* minimal polinomlarının hangi kuralı takip ettiğini bulmak o kadar da kolay değildir. Hatta bazen bu kuralı bulmaya çalışmak yerine P_q^* minimal polinomun kendisini $q \in \mathbb{N}$'nin tek ve çift olma durumuna gore hesaplamak çok daha kolaydır. Bu durum Ozgur ve arkadaşları tarafından (2012a) tarafından çalışılmıştır.

Aşağıda bu durumu anlatan örneğe yer verilmiştir. Bu örnekte yine Maple'a başvurulmuştur ancak yukarıdaki polinomlardan farklı olarak bir kural olmadığından dolayısı ile bir döngü de söz konusu değildir. Belli kurala uymayan bu polinomların φ Euler fonksiyonuna, ψ_n minimal polinomlarına ve D_n Dickson polinomlarına bağlı olduğuna dikkat edilmelidir. Dolayısıyla Maple'da φ Euler fonksiyonunun hesaplanması için "with(numtheory)" adlı paket ve ψ_n minimal polinomlarınının hesaplanması için "with(orthopoly)" adlı paketler çağrılmalıdır. Dickson Polinomlarının hesaplanması için de (2.2)'deki tanım kullanılarak bu polinomlar MAPLE'da ifade edilmelidir. Tüm bu hazırlıklardan sonra istenilen minimal polinom hesaplanmaya hazır hale gelir.

Örnek 4.3.6. $q = 300$ için $P_{300}^*(x) = ?$

$q = 300$ çift olmak üzere Teorem 2.5.5'in (2.6) eşitliği kullanılırsa

$q = 300$ için
$$P_{300}^*(x) = 2^{\frac{\varphi(600)-300}{2}} \cdot \frac{D_{301}(x) - D_{299}(x)}{\prod_{\substack{d|600 \\ d \neq 600 \\ d \nmid 300}} \psi_d\left(\frac{x}{2}\right).[D_{151}(x) - D_{149}(x)]} \tag{2.74}$$

eşitliği alınır. (3.74)'teki çarpım sembolü altındaki şartlar düşünüldüğünde $d|600$'ün d bölenlerini Maple'da "with(numtheory)" adlı paketin içinde "divisors" isimli paket ile hesaplanmaktadır. Buna göre d bölenleri Maple'da

```
> with(numtheory):
> divisors(600);
```

{ 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 25, 30, 40, 50, 60, 75, 100, 120, 150, 200, 300, 600 }

şeklinde sıralanır. $d \nmid 300$ koşuluna uyan bölenler ise Maple'da

```
> divisors(300);
```

{ 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 25, 30, 50, 60, 75, 100, 150, 300 }

biçiminde sıralanır. $d \nmid 300$ ve $d \neq 600$ koşulları $d|600$ bölenlerinde göz önüne alınırsa d bölenleri 8, 24, 40, 120, 200 olarak bulunur. Bu bölenler, (3.74)'teki çarpım sembolü için düşünüldüğünde

$$\prod_{\substack{d|600 \\ d\neq 600 \\ d\nmid 300}} \psi_d\left(\frac{x}{2}\right) = \psi_8\left(\frac{x}{2}\right)\psi_{24}\left(\frac{x}{2}\right)\psi_{40}\left(\frac{x}{2}\right)\psi_{120}\left(\frac{x}{2}\right)\psi_{200}\left(\frac{x}{2}\right) \tag{3.75}$$

çarpımı elde edilir. Bu çarpımdaki her bir ψ_n Minimal polinomların hesabı için $n \in \mathbb{N}$ çift olmak üzere Teorem 2.4.1'in (2.4) eşitliği kullanılmalıdır. Buna göre Örnek 3.2.6'nın (3.43) eşitliğinden ψ_{200} minimal polinomu

$$n = 200 \text{ için} \qquad \frac{(T_{101}(x)-T_{99}(x))(T_{11}(x)-T_9(x))}{2^{40}(T_{51}(x)-T_{49}(x))(T_{21}(x)-T_{19}(x))} = \psi_{200}(x) \tag{3.76}$$

şeklinde bulunur. Benzer şekilde ψ_{120} minimal polinomunda

$$n = 120 = 2.60 \text{ için} \qquad T_{61}(x) - T_{59}(x) = 2^{60}\prod_{d|120}\psi_d(x) \tag{3.77}$$

eşitliği alınır. (3.77)'de $d|120$ bölenleri Maple'da

```
> divisors(120);
```

{ 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120 }

olarak sıralanır. Bu bölenler (3.77)'de ele alındığında

$$T_{61}(x) - T_{59}(x) = 2^{60}\psi_1(x)\psi_2(x)\psi_3(x)\psi_4(x)\psi_5(x)\psi_6(x)\psi_8(x)\psi_{10}(x) \\ \psi_{12}(x)\psi_{15}(x)\psi_{20}(x)\psi_{24}(x)\psi_{30}(x)\psi_{40}(x)\psi_{60}(x)\psi_{120}(x) \tag{3.78}$$

eşitliği elde edilir. (3.78)'de

$n = 60 = 2.30$ için

$$T_{31}(x) - T_{29}(x) = 2^{30}\prod_{d|60}\psi_d(x)$$

$$T_{31}(x) - T_{29}(x) = 2^{30}\psi_1(x)\psi_2(x)\psi_3(x)\psi_4(x)\psi_5(x)\psi_6(x) \\ \psi_{10}(x)\psi_{12}(x)\psi_{15}(x)\psi_{20}(x)\psi_{30}(x)\psi_{60}(x) \tag{3.79}$$

eşitliği alınır. (3.79), (3.78)'de ele alınırsa

$$\frac{T_{61}(x)-T_{59}(x)}{2^{30}[T_{31}(x)-T_{29}(x)]} = \psi_8(x)\psi_{24}(x)\psi_{40}(x)\psi_{120}(x) \tag{3.80}$$

eşitliği elde edilir. Dikkat edilirse (3.80)'deki çarpım (3.78)'de aynen bulunmaktadır. Bu sebeple (3.80) ve (3.76) eşitlliklerini kullanmak ψ_n'lerin çarpımı için yeterli olacaktır. O halde

$$\prod_{\substack{d|600 \\ d\neq 600 \\ d\nmid 300}} \psi_d\left(\frac{x}{2}\right) = \psi_8\left(\frac{x}{2}\right)\psi_{24}\left(\frac{x}{2}\right)\psi_{40}\left(\frac{x}{2}\right)\psi_{120}\left(\frac{x}{2}\right)\psi_{200}\left(\frac{x}{2}\right)$$

$$= \frac{(T_{101}(x)-T_{99}(x))(T_{11}(x)-T_9(x))(T_{61}(x)-T_{59}(x))}{2^{70}(T_{51}(x)-T_{49}(x))(T_{21}(x)-T_{19}(x))(T_{31}(x)-T_{29}(x))} \tag{3.81}$$

eşitliği MAPLE'da hesaplanıp $x = x/2$ için değişken değişimi yapılmalıdır.

(3.74)'te $\varphi(600)$'ün hesabı Maple'da da yapılabilir. Bunun için "with(numtheory)" adlı paket çağrılmalıdır.

```
> with(numtheory);
```

$[GIgcd, bigomega, cfrac, cfracpol, cyclotomic, divisors, factorEQ, factorset, fermat, imagunit, index, integral\_basis, invcfrac, invphi, iscyclotomic, issqrfree, ithrational, jacobi, kronecker, \lambda, legendre, mcombine, mersenne, migcdex, minkowski, mipolys, mlog, mobius, mroot, msqrt, nearestp, nthconver, nthdenom, nthnumer, nthpow, order, pdexpand, \phi, \pi, pprimroot, primroot, quadres, rootsunity, safeprime, \sigma, sq2factor, sum2sqr, \tau, thue]$

```
> phi(600);
```

$$160$$

$q = 300$ için $\qquad P^*_{300}(x) = 2^{-70}.\dfrac{D_{301}(x)-D_{299}(x)}{\prod_{\substack{d|600 \\ d\neq 600 \\ d\nmid 300}} \psi_d\left(\frac{x}{2}\right).[D_{151}(x)-D_{149}(x)]}$

minimal polinomunun MAPLE ile hesaplanışı aşağıdadır.

```
> with(numtheory):
> phi(300);
```

$$80$$

```
> with(orthopoly):
>evala(Divide(sort(expand((T(101,x)-T(99,x))*(T(11,x)-
T(9,x))*(T(61,x)-T(59,x)))),sort(expand((T(51,x)-
T(49,x))*(T(21,x)-T(19,x))*(T(31,x)-T(29,x)))),'q'));
```

$$true$$

```
> A:=subs(x=x/2,sort(q));
```

$$A := x^{70} - 70\,x^{68} + 2345\,x^{66} - 50050\,x^{64} + 764400\,x^{62} - 8895264\,x^{60} + 82003215\,x^{58} - 614745190\,x^{56} + 3817369325\,x^{54} - 19900384350\,x^{52} + 87959698826\,x^{50} - 332051251300\,x^{48} + 1076304054925\,x^{46} - 3006679329750\,x^{44} + 7255914777375\,x^{42} - 15145072038950\,x^{40} + 27345263388625\,x^{38} - 42671939891750\,x^{36} + 57442905936250\,x^{34} - 66512573902500\,x^{32} + 65979837565885\,x^{30} - 55783449376550\,x^{28} + 39933854402175\,x^{26} - 24009358813750\,x^{24} + 12001813860000\,x^{22} - 4926270325152\,x^{20} + 1634648793665\,x^{18} - 429924307090\,x^{16} + 87364199725\,x^{14} - 13258314550\,x^{12} + 1433608033\,x^{10} - 103146330\,x^{8} + 4443655\,x^{6} - 96650\,x^{4} + 825\,x^{2} - 2$$

```
>print(300,evala(Divide(((sort(sum((-1)^i*301*(301-1-
i)!/(301-2*i)!*1/i!*x^(301-2*i),i=0..floor(301/2))))-
(sort(sum((-1)^i*299*(299-1-i)!/(299-2*i)!*1/i!*x^(299-
```

```
2*i),i=0..floor(299/2))))),expand(A*((sort(sum((-
1)^i*151*(151-1-i)!/(151-2*i)!*1/i!*x^(151-
2*i),i=0..floor(151/2))))-(sort(sum((-1)^i*149*(149-1-
i)!/(149-2*i)!*1/i!*x^(149-
2*i),i=0..floor(149/2)))))),'q1')),sort(q1));
```

$$300, \mathit{true}, x^{80} - 80\, x^{78} + 3080\, x^{76} - 76000\, x^{74} + 1350500\, x^{72} - 18410016\, x^{70} + 200271120\, x^{68} - 1785587520\, x^{66} + 13298907050\, x^{64} - 83914230400\, x^{62} + 453376599105\, x^{60} - 2114562794300\, x^{58} + 8567088969550\, x^{56} - 30294642994000\, x^{54} + 93834706195125\, x^{52} - 255230403575364\, x^{50} + 610658700046325\, x^{48} - 1286317599865200\, x^{46} + 2385912221810250\, x^{44} - 3894864908627000\, x^{42} + 5589138334474464\, x^{40} - 7037191909138560\, x^{38} + 7754194971956485\, x^{36} - 7452640256210100\, x^{34} + 6221786745606300\, x^{32} - 4488970420294784\, x^{30} + 2781910284102770\, x^{28} - 1469975927142520\, x^{26} + 656482177035500\, x^{24} - 245185119524000\, x^{22} + 75613509383565\, x^{20} - 18960032631300\, x^{18} + 3793197271675\, x^{16} - 591424702000\, x^{14} + 69756766625\, x^{12} - 5986147596\, x^{10} + 354277210\, x^{8} - 13353360\, x^{6} + 279800\, x^{4} - 2400\, x^{2} + 1$$

KAYNAKLAR

Cangul, I. N. 1993. Normal Subgroups of Hecke Groups. PhD Thesis, Faculty of Mathematical Studies, University of Southampton, England.

Evans, R. 1973. A Fundamental Region for Hecke's Modular Group. *J. of No. Thry.*, 5: 108-115.

Fraleigh, J. B. 1974. A First Course in Abstract Algebra. sixth ed., Addison-Wesley Pub. Comp. 536 pp.

Fraleigh, J. B. 2002. A First Course in Abstract Algebra. seventh ed., Addison-Wesley Pub. Comp. 590 pp.

Jones, G. A., Jones, J. M. 2005. Elemantary Number Theory. eigth ed., Springer Science + Business Media, LLC, New York, USA, 301 pp.

Grillet, P. E. 2007. Abstract Algebra. Second ed., Springer Science + Business Media, LLC, New York, USA, 669 pp.

Hecke, E. 1936. Über die Bestimmung Dirichletscher Reichen durch ihre Funktionalgleichungen. *Math. Ann.*, 112: 664-699.

Kurur, P. 2007. Computational Number Theory Lecture Notes. Chennai Mathematical Institute, India, http://www.cmi.ac.in/~ramprasad/lecturenotes/index.php?notes=cnt – (15.10.2012).

Lehner, J. 1964. Discontinuous Groups and Automorphic Forms. Math. Surveys, 8, A.M.S. Providence, R.I.

Macbeath, A. M. 1969. Generators of the Lineer Fractional Groups. *Proc. Symp. Pure Math., A.M.S.*, 12: 14-32.

Maclachlan, C. 1971. Maximal Normal Fuchsian Groups. *Illionis J. Math.*, 15: 104-113.

Mc Quillan, D. L. 1965. Classification of Normal Subgroups of the Modular Group. *Illionis of J. Math.*, 6: 285-296.

Newman, M. 1967. Classification of Normal Subgroups of the Modular Group. *Trans. A.M.S.,* 126: 267-277.

Ozgur, B., Cangul, I. N., 2012a. The Minimal Polynomial of Some Trigonometric Numbers over $\mathbb{Q}$. International Congress in Honour of Professor H. M. Srivastava, 23 - 26 August 2012, Uludag University, Bursa.

Ozgur, B., Yurttas, A., Cangul, I. N., 2012b. Determing the minimal polynomial of $\cos(2\pi/n)$ over $\mathbb{Q}$ with Maple. *Numerical Analysis And Applied Mathematics*, *AIP Conf. Proc.* 1479: 368-370.

Yurttas, A., Ozgur, B., Cangul, I. N., 2012c. Calculation of the minimal polynomial of $\cos\ 2(\pi/n)$ over $\mathbb{Q}$ with Maple. *Numerical Analysis And Applied Mathematics*, *AIP Conf. Proc*. 1479: 371-374.

Özgür, B., Cangül, İ. N., 2011. Hecke Gruplarının Kongrüans Alt Grupları, XXIV. Ulusal Matematik Sempozyumu, 7-10 Eylül 2011, Uludağ Üniversitesi, Bursa.

Parson, L. A. 1976. Generalized Kloosterman Sums and the Fourier Coefficients of Cusps Forms. *Trans. A.M.S*., 217: 329-350.

Parson, L. A. 1977. Normal Congruence Subgroups of the Hecke Groups $G\left(2^{(1/2)}\right)$ and $G\left(3^{(1/2)}\right)$. *Pasific J. of Math.,*70: 481-487.

Rosen, D. 1963. An Arithmetic Characterization of the Parabolic Points of $G(2cos\pi/5)$. *Proc. Glasgow Math. Assoc*., 6: 88-96.

Togan, M., Ozgur, B., Cangul, I. N., 2011c. Some Special Cases of the Minimal Polynomial of $2\cos(\pi/q)$ over Q**.** *Numerical Analysis And Applied Mathematics*, *AIP Conf. Proc*. 1389: 375-377**.**

Watkins, W., Zeitlin, J. 1993. The Minimal Polynomial of $cos(2\pi/n)$. *The Amer. Math. Monthly*, 100: 471-474.

Weber, H. 1898. Traite d'algebra superiure, I, Gauthier-Villars, Paris, 764 pp.