İkinci Kuvvette Karşılıklılık

Ayberk Zeytin, İbrahim Emir Çiçekli / azeytin@gsu.edu.tr,
IbrahimEmir.Cicekli@ogr.gsu.edu.tr

Bu yazıda tek bilinmeyenli tamsayı katsayılı denklemlerin çözümüyle ilgileniyor olacağız. Böyle denklemleri ilk olarak derecesine göre sınıflandırırız. Okuyucuların daha ilkokul çağlarından da hissedebileceği gibi derece yükseldikçe denklemlerin çözümleri zorlaşır. Bu noktada yardımımıza yetişen tekniklerden bir tanesi de denklemleri çeşitli modlara indirgeyerek çözmeye çalışmaktır. Örneğin, verilen a ve b tamsayıları için $ax + b = 0$ şeklinde bir denkleminin $-b/a$ şeklinde verilen rasyonel çözümü yerine modülo m'de çözmeye çalışabiliriz. Bu durumda, dikkatli okuyucunun da hemen farkına varacağı üzere bu denklemin modülo m'de çözümü $x = -b/a$ yerine $x = -ba^{-1}$ şeklinde ifade edilir ki buradan da hemen a'nın modülo m'de çarpmaya göre tersinin olmasının gerekliliği (ve yeterliliği) görülür. Bu da elbette ki a ile m'nin aralarında asal olmasına denktir.

Dereceye göre tasnifte bir sonraki durum ikinci dereceden denklemler. Verilen a, b, c tamsayıları için $ax^2 + bx + c = 0$ şeklindeki tamsayı katsayılı deklemlerinin çözümü, hepimizin aşina olduğu $\dfrac{-b \pm \sqrt{\Delta}}{2a}$ ile verilir. Bu çözümü birinci derece olduğu gibi modülo m'de ifade edilmesi esnasında en büyük engelin karekök fonksiyonu olduğu hemen göze çarpar. Bu yazıda bu problemi biraz daha genel bir perspektiften ele alacağız. Elde ettiğimiz sonuçları ikinci kuvvette karşılıklılığı ispatlamak üzere kullanacağız. İspatımızda geçecek olan karakterler ve Gauss toplamları gibi bazı kavramlara derinine inmeden değineceğiz. Her iki konunun da ayrı yazılarda detaylandırılmayı hakettiğini düşünüyoruz.

1 Grup Karakterleri

Bu bölümde başrol oyuncusu $\mathbb{Z}/m\mathbb{Z}$ halkası olacak. Bu halkanın çarpma işlemi altında tersinir elemanlarını kümesini $(\mathbb{Z}/m\mathbb{Z})^\times$ ile gösterelim. Bu küme çarpma işlemi altında bir gruptur. Aşağıda bu grubun karakterlerini tanımlayacağız. Bu karakterleri tamsayılar kümesine genişleterek Dirichlet karakterlerini elde edeceğiz.

Tanım. m bir doğal sayı olsun. $(\mathbb{Z}/m\mathbb{Z})^\times$ grubundan $\mathbb{C}^\times$ grubuna tanımlı her homomorfiye bir *karakter*, ya da belirtilmesi gerekli olduğu durumda *modülo m'de bir karakter* denir. Modülo m'deki karakterlerin kümesini

$$X(m) := \mathrm{Hom}((\mathbb{Z}/m\mathbb{Z})^\times, \mathbb{C}^\times)$$

ile göstereceğiz.

Örneğin, modülo 2'de sadece 1 tane karakter var, zira $(\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{1}\}$. Modülo 3'de bakacak olursak iki karakter göreceğiz $((\mathbb{Z}/3\mathbb{Z})^\times = \{\overline{1}, \overline{2}\})$: her elemanı 1'e gönderen $\mathbb{1}_3$ homomorfisi ve $\overline{1}$'i 1'e ve $\overline{2}$'yi -1'e gönderen χ_3.

$X(m)$ kümesi içinde verilen herhangi χ, χ' için,

$$(\chi \cdot \chi')(x) := \chi(x)\chi'(x)$$

(noktasal çarpma) işlemini tanımlayabiliriz. Yukarıda modülo üç için tarif edilen χ_3 karakterine bakacak olursak :

$$\begin{aligned} \mathbb{1} \cdot \chi_3 &= \chi_3, \text{ ve} \\ \chi_3 \cdot \chi_3 &= \mathbb{1} \end{aligned}$$

eşitliklerini görebiliriz. Verilen herhangi iki karakter için :

$$\begin{aligned} (\chi \cdot \chi')(xy) &= \chi(xy)\chi'(xy) \\ &= \chi(x)\chi(y)\chi'(x)\chi'(y) \\ &= \chi(x)\chi'(x)\chi(y)\chi'(y) \\ &= (\chi \cdot \chi')(x)(\chi \cdot \chi')(y). \end{aligned}$$

Dolayısıyla iki karakterin çarpımı da gerçekten bir karakterdir. Okuyucunun da tahmin edeceği üzere :

Teorem 1. *$X(m)$ kümesi yukarıda tanımlanan noktasal çarpma işlemi altında bir abelyen gruptur.*

Kanıt. Birleşme özelliği, işlemimizin tanımı gereği, $\mathbb{C}^\times$'de çarpmanın birleşme özelliğinden geliyor. Bunu yazmayı okura bırakıyoruz. Birim elemanımız $\mathbb{1}(x) := 1$ olarak tanımlanan birim homomorfimiz. Herhangi bir karakter $\chi \in X(m)$'in tersi ne olmalı? Diyelim ki bu ters eleman $\psi \in X(m)$ ile gösterilsin. Her x için,

$$(\chi \cdot \psi)(x) = \chi(x)\psi(x) = 1 \Leftrightarrow \psi(x) = 1/\chi(x).$$

Yani $\psi(x) = \frac{1}{\chi(x)} \in X(m)$ bizim χ karakterimizin tersiymiş. ψ'yi χ^{-1} olarak gösterelim. Ancak bu ψ'yi daha detaylı incelemekte fayda var.

Mertebesi d olan herhangi bir $t \in (\mathbb{Z}/m\mathbb{Z})^\times$ için $1 = \psi(1) = \psi(t^d) = \psi(t)^d$ olacağından, $\psi(t)$,

x^d-1 polinomunun bir köküdür. Yani her elemanın ψ altında görüntüsü bir d için x^d-1 şeklindeki bir polinomun kökü olacak. Ancak bu geometrik olarak, karakterler grubun elemanlarını karmaşık düzlemde orijin merkezli birim çembere gönderiyor demek. Yani her x için, $|\psi(x)| = 1$.

O zaman,

$$\chi^{-1}(x) = \frac{1}{\chi(x)} = \frac{\overline{\chi(x)}}{\chi(x)\overline{\chi(x)}} = \frac{\overline{\chi(x)}}{|\chi(x)|^2} = \overline{\chi(x)}.$$

Yani χ karakterinin tersi tamı tamına χ karakterinin karmaşık eşleniğiymiş. Bundan ötürü karakterlerin terslerini karmaşık eşlenik sembolüyle göstereceğiz.

Grubun değişme özelliği karakterlerin görüntü kümesi $\mathbb{C}^\times$'in değişme özelliğinden gelir.

Eğer χ karakterinin mertebesi 2 ise, yani $\chi(t) \in \{\pm 1\}$ ve $\chi(t) \neq \mathbb{1}$ ise, χ'ya **kuadratik** karakter diyelim. Örneğin, $(\mathbb{Z}/5\mathbb{Z})^\times$ grubu 2 tarafından üretilir. Dolayısıyla $\varphi : (\mathbb{Z}/5\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ fonksiyonu $t = 2^k \mapsto (-1)^k$ kuralıyla tanımlanırsa bir homomorfi ve dolayısıyla bir kuadratik karakter olacaktır.

Birazdan listeleyeceğimiz sonuçların bir kısmı $(\mathbb{Z}/m\mathbb{Z})^\times$ grubunun döngüsel olmasına dayanıyor. Ancak bu grup her zaman döngüsel değil. Örneğin $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, zira gruptaki birimden farklı her üç elemanın da mertebesi 2. Okuyucunun $(\mathbb{Z}/m\mathbb{Z})^\times$ grubunun döngüsel olmasi için p tek bir asal sayı ve k bir pozitif tamsayı belirtmek üzere $m = 1, 2, 4, p^k, 2p^k$ koşulunun gerek ve yeterli olduğuna inanmasını isteyelim. Meraklı okuyucu bir ispat için Gauss'un meşhur "Disquisitiones Arithmeticae" kitabında ispatı arayabilir. Akışı bozmamak adına buradan itibaren $m = 1, 2, 4, p^k, 2p^k$ olarak kabul edeceğiz.

1. $X(m)$'in mertebesi nedir? Öncelikle döngüsel gruplar üzerinde tanımlı homomorfilerin, üreteçlerinin görüntüsü tarafından belirlendiğini fark edelim. Diyelim ki $(\mathbb{Z}/m\mathbb{Z})^\times$ grubu ω ile üretiliyor. Herhangi bir $x \in (\mathbb{Z}/m\mathbb{Z})^\times$, ω cinsinden $x = w^t$ olarak yazılsın. Öyleyse

$$\chi(x) = \chi(w^t) = \chi(w)^t$$

olur. Homomorfinin üretecin görüntüsü tarafından belirlenmesi demek, bir homomorfi yazarken üreteci nereye gönderdiğini söylediğin anda homomorfi belirlendi demek. Dolayısıyla üretecin gidebileceği görüntü sayısı kadar muhtemel homomorfi var.

Bir önceki ispatımızda her elemanın χ altında görüntüsü bir d için x^d-1 şeklindeki bir polinomun kökü olacak demiştik. Bu durumda üreteci göz önünde bulundurduğumuza göre d'miz $(\mathbb{Z}/m\mathbb{Z})^\times$'nin eleman sayısı olmalı. Bu sayı meşhur Euler'in φ fonksiyonuyla gösterilir. $\varphi(m)$ fonksiyonu m ile aralarında asal ve m'den küçük doğal sayıların adedini verir. Bu da tamı tamına $(\mathbb{Z}/m\mathbb{Z})^\times$ grubunun eleman sayısıdır. Yani χ karakteri ω elemanını, $x^{\varphi(m)}-1$ polinomun köklerinden birine gönderiyor. Karmaşık sayılarda bu polinomun $\varphi(m)$ tane kökü var. Bu da ω üretecinin muhtemel $\varphi(m)$ görüntüsü var demek. Her bir ihtimal bir homomorfi verdiğine göre $\#X(m) = \varphi(m)$.

2. $X(m)$ kümesinin elemanlarının $\mathbb{Z}$'ye doğal bir genişlemesi var. Buna da χ ile ilişkili modülo m Dirichlet karakteri deniyor ve şöyle tanımlanıyor: Herhangi bir $a \in \mathbb{Z}$ için,

$$\tilde{\chi}(a) = \begin{cases} \chi(a + m\mathbb{Z}), & \text{eğer } (a, m) = 1 \text{ ise} \\ 0, & \text{eğer } (a, m) > 1 \text{ ise} \end{cases}$$

Yani a tamsayısının modülo m'de kalan sınıfını buluyor, sonra kalan sınıfını χ ile değerlendiriyoruz.

3. Ayrıca elimizde şöyle bir eşitlik var.

$$\sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(t) = \begin{cases} \varphi(m), & \text{eğer } \chi = \mathbb{1} \text{ ise} \\ 0, & \text{eğer } \chi \neq \mathbb{1} \text{ ise} \end{cases}$$

Bu eşitliği hemen görmek mümkün. χ esas karakter olduğunda da bu toplamın grubun eleman sayısını sayacağını hemen görüyoruz. Diğer durumda, yani χ karakterinin birim karakter olmadığını varsaydığımızda en az bir $k \in (\mathbb{Z}/m\mathbb{Z})^\times$ için $\chi(k)$ sayısı 1'den farklı olmalı. O zaman grubunun her elemanını k ile çarpmak grubun elemanlarının bir permütasyonudan başka bir şey değil, dolayısıyla

$$\begin{aligned} \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(t) &= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(kt) \\ &= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(k)\chi(t) \\ &= \chi(k) \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(t). \end{aligned}$$

eşitliğini elde edeceğiz. $\chi(k) \neq 1$ olduğuna göre, toplam sıfır olmalı. Bu "elemanları kaydırma" hamlesinin bu konuda ve özellikle de bu yazıda sıkça istifade edilen bir yöntem olduğunu okura şimdiden iletelim.

Tanım. $k \mid n$ olacak şekilde k ve m doğal sayıları alalım. $\psi \in X(k)$ ve $\chi \in X(m)$ iki karakter olsun.

Eğer $(a,m)=1$ eşitliğini sağlayan her $a \in \mathbb{Z}$ için $\tilde{\chi}(a)=\tilde{\psi}(a)$ eşitliği de varsa, $\tilde{\chi}$'ya $\tilde{\psi}$'den *türetilmiş karakter* denir. Bir $\chi \in X(m)$ için, $\tilde{\chi}$, m tam sayısının öz bölenlerinden gelen hiçbir karakterden türetilemiyorsa $\tilde{\chi}$ karakterine *ilkel karakter* denir.

Misal $\chi \in X(9)$ Dirichlet karakteri şöyle tanımlanmış olsun:

$$\chi(1)=\chi(4)=\chi(7)=1$$
$$\chi(2)=\chi(5)=\chi(8)=-1$$
$$\chi(3)=\chi(6)=\chi(9)=0$$

Bariz bir şekilde 3-periyodiklik var. Dolayısıyla bu karakterin $\psi(1)=1, \psi(2)=-1, \psi(3)=0$ ile tanımlanmış $\psi \in X(3)$ karakterinden türetilmiş olduğunu görüyoruz. Eğer p bir asal sayıysa her $\chi \in X(p)$'nin ilkel karakter olduğunu doğrulamak bu tanımın anlaşılmasını sağlayacak güzel bir alıştırma olacaktır.

2 Gauss toplamları

Verilen bir tek p asal sayısı ve bir tamsayı a için Legendre sembolü :

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & (a,p)=p \text{ ise} \\ 1 & a \equiv b^2 \pmod p \\ & \text{eşitliğini sağlayacak bir} \\ & b \text{ tamsayısı var ise} \\ -1 & \text{diğer hallerde} \end{cases}$$

olarak tanımlanır. Başka bir deyişle, Legendre sembolü verilen bir tek p asal sayısı ve p ile bölünmeyen bir a tamsayısı için - yazının başında da değinildiği üzere - $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ elemanının yine aynı halka içinde karekökü var ise 1, aksi takdirde -1 sonucu vermektedir. Ya da daha gayrı resmi bir dille ifade etmek gerekirse $(a,p) \neq p$ ise

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow \sqrt{a} \in \mathbb{Z}/p\mathbb{Z}.$$

Hatırlanacağı üzere p bir tek asal, ve dolayısıyla $(\mathbb{Z}/p\mathbb{Z})^\times$ grubu döngüsel. $(\mathbb{Z}/p\mathbb{Z})^\times = \langle \alpha \rangle$ olacak α seçecek olursak bir $k \in \{1,2,\ldots,p-1\}$ tamsayısı için $a=\alpha^k$ olmalı. Buradan hareketle :

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow k \text{ çift tamsayı , ve}$$
$$\left(\frac{a}{p}\right) = -1 \Leftrightarrow k \text{ tek tamsayı .}$$

Dolayısıyla $\mathbb{Z}/p\mathbb{Z}$ halkasında:

- eğer iki sayının karekökünü alabiliyorsak çarpımlarının da karekökünü alabiliriz,
- eğer iki sayının karekökünü alamıyorsak çarpımlarının karekökünü alabiliriz, ve
- eğer iki sayıdan birinin karekökünü alabililyor ancak diğerinin alamıyorsak, çarpımlarının karekökünü alamayız.

Yukarıdaki çıkarımlardan $\left(\frac{\cdot}{p}\right)$ ile tanımlanan Legendre sembölünün modülo p kuadratik bir karakter tanımladığını hemen görürüz. Gauss birazdan tanımlayacağımız toplamları Legendre sembolünü kullanarak tanımladı. Biz ise biraz daha genelleştirip modülo m karakterler için tanımlayacağız. Önce bir gösterim :

$$\zeta_m = e^{\frac{2\pi i}{m}} = \cos\left(\frac{2\pi}{m}\right) + i\sin\left(\frac{2\pi}{m}\right)$$

olsun. Dolayısıyla ζ_m, z^m-1 polinomunun bir köküdür.

Tanım. Herhangi bir $\chi \in X(m)$ ve $\alpha \in \mathbb{Z}/m\mathbb{Z}$ ikilisi için, (χ,α) ile ilişkili Gauss toplamı aşağıdaki gibi tanımlanır:

$$\tau(\chi,\alpha) := \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(t)\zeta_m^{\alpha t}$$

Basit bir durum için bir Gauss toplamı hesaplayarak tanımı daha iyi anlayalım. m tamsayısının bir asal - dolayısıyla $(\mathbb{Z}/m\mathbb{Z})^\times$ grubununun döngüsel - olduğunu düşünelim. Örneğin $\chi=\mathbb{1}$ ve $\alpha=1$ için,

$$\begin{aligned} \tau(\mathbb{1},1) &= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \mathbb{1}(t)\zeta_m^t \\ &= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \zeta_m^t \\ &= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} e^{\frac{2\pi i t}{m}} \\ &= \sum_{i=1}^{m-1} e^{\frac{2\pi i t}{m}} \end{aligned}$$

0'dan $m-1$'e kadar topluyor olsaydık z^m-1'in köklerini toplamış olurduk ve bu toplam da 0'a eşit olurdu. Ancak $i=0$'lı terim eksik olduğuna göre,

$$\tau(\mathbb{1},1) = \sum_{i=1}^{m-1} e^{\frac{2\pi i t}{m}} = -1$$

olmalı.

Grup karakterleri doğal bir biçimde $\mathbb{Z}$'ye genişletişebildiği gibi, Gauss toplamının tanımı da $\mathbb{Z}$' ye genişletilebiliyor. Herhangi bir $a \in \mathbb{Z}$ için,

$$\tau(\chi,a) = \tau(\chi, a+m\mathbb{Z})$$

şeklinde tanımlansın. Yani önce a'nın modülo m'de kalan sınıfını bulup ondan sonra Gauss toplamında değerlendirelim. Yazı boyunca, kafa karışıklığına sebep olmayacağını düşündüğümüz yerlerde, $\tilde{\chi}$ yerine χ yazacağız. Ayrıca, $\tau(\chi)$ yazdığımızda $\tau(\chi, 1)$ toplamını kastettiğimizde anlaşalım. Gauss toplamı üzerine üç önemli teoremimiz var.

Teorem 2. *m pozitif tamsayı, $\chi \in X(m)$ bir karakter olsun.*

χ ilkel olması m'nin her öz böleni k için, $(a, m) = 1$, $a \equiv 1 \bmod k$ ve $\tilde{\chi}(a) \neq 1$ koşullarını sağlayacak bir a tamsayısının varlığına denktir.

Kanıt. Varsayalım ki $(a, m) = 1$ ve $a \equiv 1 \bmod k$ eşitliklerini sağlayan her $a \in \mathbb{Z}$ için $\tilde{\chi}(a) = 1$ olacak şekilde bir $k \mid m$ öz böleni var. Şu örten homomorfiyi inceleyelim. Her $(a, m) = 1$ olacak şekilde a tamsayısı için,

$$\begin{aligned} \pi : (\mathbb{Z}/m\mathbb{Z})^\times &\longrightarrow (\mathbb{Z}/k\mathbb{Z})^\times \\ a + m\mathbb{Z} &\mapsto a + k\mathbb{Z} \end{aligned}$$

Bu homomorfinin çekirdeği elbette

$$\ker(\pi) = \{a + m\mathbb{Z} | (a, m) = 1 \text{ ve } a \equiv 1 \bmod k\}$$

olacaktır. Ancak bu durumda çekirdekteki her $a + m\mathbb{Z}$ için, $\tilde{\chi}(a) = 1$ olacak. Yani $\ker(\pi) \subset \ker(\chi)$. Öyleyse iddia ediyoruz ki $\psi \circ \pi = \chi$ olacak şekilde bir $\psi\colon (\mathbb{Z}/k\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ homomorfisi vardır. Bu homomorfinin varlığını gösterebilirsek her $a \in \mathbb{Z}$,$(a, m) = 1$ için $\psi(a) = \chi(a)$ olacak şekilde bir $\psi \in X(k)$ bulmuş olacağız. Yani χ, ψ'den türetilmiş olacak. Diyagramımıza bakalım.

$$\begin{tikzcd} (\mathbb{Z}/m\mathbb{Z})^\times \arrow[rr, two heads, "\pi"] \arrow[dr, "\chi"'] & & (\mathbb{Z}/k\mathbb{Z})^\times \arrow[dl, dotted, "\exists?\ \psi"] \\ & \mathbb{C}^\times & \end{tikzcd}$$

$\psi \circ \pi = \chi$ olacak şekilde bir ψ arıyoruz. $(\mathbb{Z}/k\mathbb{Z})^\times$'da herhangi bir y elemanı alalım. π örten olduğuna göre $\pi(x) = y$ olacak şekilde bir $x \in (\mathbb{Z}/m\mathbb{Z})^\times$ var. O zaman ψ'yi $\psi(y) := \chi(x)$ olacak şekilde tanımlayalım. Tanım gereği $x \in (\mathbb{Z}/k\mathbb{Z})^\times$ için, tam da istediğimiz gibi $\psi(\pi(x)) = \chi(x)$ olur. Ancak $\pi(x) = y$ eşitliğini sağlayan birden fazla x olabilir. Dolayısıyla bu ψ fonksiyonunun iyi tanımlı olduğunu doğrulamalı. Yani $x_1, x_2 \in (\mathbb{Z}/k\mathbb{Z})^\times$ için, $\pi(x_1) = \pi(x_2)$ ise, $\chi(x_1) = \chi(x_2)$ olmalı.

$$\begin{aligned} &\pi(x_1) = \pi(x_2) \\ &\Rightarrow \pi(x_1)\pi(x_2)^{-1} = 1 \\ &\Rightarrow \pi(x_1 x_2^{-1}) = 1 \\ &\Rightarrow x_1 x_2^{-1} \in \ker(\pi) \end{aligned}$$

Öte yandan $\ker(\pi) \subset \ker(\chi)$ olduğunu görmüştük. Yani $x_1 x_2^{-1} \in \ker(\chi)$ oldu. O zaman $\chi(x_1 x_2^{-1}) = 1$ yani $\chi(x_1) = \chi(x_2)$.

Şimdi ise χ karakterinin ilkel olmadığını varsayalım. m'nin öz bir böleni k ve $(a, m) = 1$, $a \equiv 1 \bmod k$ özelliklerini sağlayan her $a \in \mathbb{Z}$ için, $\chi(a) = 1$ olduğunu göstereceğiz. İspatın bu yönü nispeten daha kolay. χ ilkel olmadığına göre bir $k \mid n$ ve her $(a, m) = 1$ olacak a için $\tilde{\chi}(a) = \tilde{\psi}(a)$ olacak şekilde bir $\psi \in X(k)$ var. Öte yandan $a \equiv 1 \bmod k$ ise,

$$\tilde{\chi}(a) = \chi(a + m\mathbb{Z}) = \psi(a + k\mathbb{Z}) = \psi(1 + k\mathbb{Z}) = 1$$

İlk iddiada gösterilmek istenen de buydu.

Teorem 3. *a tamsayısı için, $\overline{\tau(\chi, a)} = \tilde{\chi}(-1)\tau(\overline{\chi}, a)$. Ayrıca $(a, m) = 1$ ise veya χ ilkelse $\tau(\chi, a) = \overline{\chi}(a)\tau(\chi)$.*

Kanıt.

$$\overline{\tilde{\chi}(-1)}\tilde{\chi}(-1) = \tilde{\chi}(-1)\tilde{\chi}(-1) = \tilde{\chi}(1) = 1$$

olduğundan $\overline{\tilde{\chi}(-1)} = \tilde{\chi}(1)$ olduğunu görebiliriz. O zaman

$$\begin{aligned} \overline{\tau(\chi, a)} &= \overline{\sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(t) e^{\frac{2\pi i}{m} at}} \\ &= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(t) e^{\frac{2\pi i}{m} at}} \\ &= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(t)} e^{-\frac{2\pi i}{m} at} \end{aligned}$$

Eğer $t + m\mathbb{Z} \mapsto -t + m\mathbb{Z}$ dönüşümünü yaparsak, $(\mathbb{Z}/m\mathbb{Z})^\times$ grubunun bir permütasyonu olduğundan, toplam değişmez. Yani,

$$\begin{aligned} \overline{\tau(\chi, a)} &= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(t)} e^{-\frac{2\pi i}{m} at} \\ &= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(-t)} e^{\frac{2\pi i}{m} at} \\ &= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(-1)\chi(t)} e^{\frac{2\pi i}{m} at} \\ &= \overline{\chi(-1)} \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(t)} e^{\frac{2\pi i}{m} at} \\ &= \chi(-1) \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(t)} e^{\frac{2\pi i}{m} at} \\ &= \chi(-1)\tau(\overline{\chi}, a) \end{aligned}$$

Benzer bir şekilde, $(a, m) = 1$ ise $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$ olacağından, $t + m\mathbb{Z} \mapsto a^{-1}t + m\mathbb{Z}$ de bir permütasyondur. Dolayısıyla,

$$\begin{aligned}\tau(\chi,a) &= \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(t)e^{\frac{2\pi i}{m}at}\\ &= \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a^{-1}t)e^{\frac{2\pi i}{m}aa^{-1}t}\\ &= \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a^{-1})\chi(t)e^{\frac{2\pi i}{m}t}\\ &= \chi(a^{-1})\sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(t)e^{\frac{2\pi i}{m}t}\\ &= \chi(a)^{-1}\sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(t)e^{\frac{2\pi i}{m}t}\\ &= \overline{\chi(a)}\sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(t)e^{\frac{2\pi i}{m}t}\\ &= \overline{\chi(a)}\tau(\chi)\end{aligned}$$

Yok eğer χ ilkel ve $(a,m)=q>1$ ise, $\tilde{\chi}(a)=0$ olur. Dolayısıyla eşitlik için $\tau(\chi,a)=0$ olduğunu göstermek yeterli. a ve m sayılarının en büyük ortak böleni q olduğuna göre, $a=qb$ ve $m=qk$ olacak şekilde b,k doğal sayıları vardır. İspatladığımız 2. iddiaya göre de öyle bir c tamsayısı var ki $(a,c)=1$, $c\equiv 1 \bmod k$ ve $\tilde{\chi}(c)\neq 1$. Şimdi tüm $t\in(\mathbb{Z}/m\mathbb{Z})^\times$ için,

$$\begin{aligned}\zeta_m^{at} &= e^{\frac{2\pi i}{m}at} = e^{\frac{2\pi i}{qk}qbt}\\ &= e^{\frac{2\pi i}{k}bt} = e^{\frac{2\pi i}{k}btc}\\ &= e^{\frac{2\pi ii}{qk}qbtc} = e^{\frac{2\pi i}{m}atc} = \zeta_m^{act}\end{aligned}$$

olduğuna göre elimizde

$$\begin{aligned}\chi(c)\tau(\chi,a) &= \chi(c)\sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(t)e^{\frac{2\pi i}{m}at}\\ &= \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(c)\chi(t)e^{\frac{2\pi i}{m}at}\\ &= \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(ct)e^{\frac{2\pi i}{m}at}\\ &= \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(ct)e^{\frac{2\pi i}{m}act}\\ &= \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(t)e^{\frac{2\pi i}{m}at} = \tau(\chi,a)\end{aligned}$$

eşitliği mevcut. $\chi(c)\neq 1$ olduğuna göre, tek ihtimal $\tau(\chi,a)=0$ olması.

Teorem 4. *χ ilkelse $|\tau(\chi)|=\sqrt{m}$ ve $\tau(\chi)\tau(\overline{\chi})=\tilde{\chi}(-1)m$.*

Kanıt. $|\tau(\chi)|$'yi hesaplayalım.

$$\begin{aligned}|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)} &= \tau(\chi)\sum_{k=0}^{m-1}\overline{\chi}(k)\zeta_m^{-k}\\ &= \sum_{k=0}^{m-1}\tau(\chi)\overline{\chi}(k)\zeta_m^{-k}\\ &= \sum_{k=0}^{m-1}\tau(\chi,k)\zeta_m^{-k}\\ &= \sum_{k=0}^{m-1}\sum_{j=0}^{m-1}\chi(j)\zeta_m^{kj}\zeta_m^{-k}\end{aligned}$$

Buradaki ikinci toplam aşağıdaki gibi kolayca hesaplanabilir :

$$\sum_{k=0}^{m-1}\zeta_m^{k(j-1)} = \begin{cases} m & j=1\\ 0 & j\neq 1\end{cases}$$

Aslına bakılırsa bu küçük iddia $j=1$ olduğu durumda kolayca görülebilir. $j\neq 1$ olduğu durumda, $u=\zeta_m^{j-1}\neq 1$ ve $u^m=1$ olacaktır.

$$S=\sum_{k=0}^{m-1}\zeta_m^{k(j-1)} \quad = (1+u+u^2+\dots u^{m-1})$$

dersek $(1-u)S=(1-u^m)=0$ elde edilir. $u\neq 1$ olduğundan $S=0$ olmalıdır. Dolayısıyla

$$\begin{aligned}\chi(c)\tau(\chi,a) &= \sum_{j=0}^{m-1}\left[\chi(j)\sum_{k=0}^{m-1}\zeta_m^{k(j-1)}\right]\\ &= \chi(1)\sum_{k=0}^{m-1}1\\ &= m\end{aligned}$$

Dolayısıyla, $|\tau(\chi)|=\sqrt{m}$ ve $m=|\tau(\chi)|^2=\tau(\chi)\overline{\tau(\chi)}=\chi(-1)\tau(\chi)\tau(\overline{\chi})$. Yani $\chi(-1)m=\tau(\chi)\tau(\overline{\chi})$. Böylece üçüncü iddiamızı ispatlamış ve dolayısıyla Gauss toplamları ile ilgili teoremlerimizi kanıtlamış olduk.

3 İkinci Kuvvette Karşılıklılık

Nihayet yazımızın ana teoremini sunacağımız bölüme geldik. Buraya kadar yapmış olduğumuz hazırlık bize karşılıklılık teoremini ispatlamada yardımcı olacak.

Teorem 5. *(Euler Kıstası) Bir p tek asal sayısı ve a tamsayısı için*

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$$

Kanıt. Verilen a tamsayısının p'nin katı olduğu durumda iddia edilen denkliğin sağlandığı kolayca görülebilir. Öyleyse $a \notin p\mathbb{Z}$ varsayabiliriz. Legendre sembolünün tanımı bize :

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow \text{ öyle bir } \alpha \in \mathbb{Z}, \quad \text{vardır ki } a \equiv \alpha^2 \pmod p$$

denkliğini verecektir. Bu da aşağıdaki diziye yol açacaktır :

$$a^{\frac{p-1}{2}} \equiv (\alpha^2)^{\frac{p-1}{2}} \equiv \alpha^{p-1} \equiv 1 \pmod p,$$

zira $({}^{\mathbb{Z}}/_{p\mathbb{Z}})^\times$ eleman sayısı $p-1$ olan döngüsel bir grup. ki bu da gösterilmek istenen iddia idi.

Ana teoremimizi sunmaya çok yakınız. Sadece iki tane yardımcı teoremimiz kaldı.

Teorem 6. *p tek asal sayı, m, p'nin katı olmayan bir tamsayı ve $\chi \in X(m)$ ilkel gerçel karakter olsun. O halde*

$$\chi(p) = \left(\frac{\chi(-1)m}{p}\right)$$

eşitliği geçerlidir.

Kanıt. Öncelikle şunu gözlemeyelim. χ kuadratik karakter ve $2 \mid p-1$ olduğuna göre $\chi^{p-1} = 1$ yani $\chi^p = \chi$. Yine aynı sebepten $\chi\overline{\chi} = 1 = \chi^2$ eşitliği var. Buradan da $\chi = \overline{\chi}$ çıkar. Yani $\chi^p = \chi = \overline{\chi}$. Gauss toplamı tam da bu noktada işimize yarayacak. $\tau(\chi)^p$'yi modülo p'de hesaplayacağız.

$\tau(\chi)^p = (\sum_{t\in({}^{\mathbb{Z}}/_{m\mathbb{Z}})^\times} \chi(t)\zeta_m^t)^p$. Bu noktada multinom açılımı imdadımıza yetişiyor. Ama önce biraz değişken değiştirelim. $\#({}^{\mathbb{Z}}/_{m\mathbb{Z}})^\times = d$ olsun. $({}^{\mathbb{Z}}/_{m\mathbb{Z}})^\times$ 'deki t'leri $\{t_1, t_2, \ldots, t_d\}$ diye numaralandıralım. $\chi(t_i)\zeta_m^{t_i} = x_i$ olsun. Toplamımız:

$$\left(\sum_{t\in({}^{\mathbb{Z}}/_{m\mathbb{Z}})^\times} \chi(t)\zeta_m^t\right)^p = \left(\sum_{i=1}^{d} x_i\right)^p$$

oldu. Multinom açılımını kullanarak toplamın

$$\sum_{b_1+b_2+\cdots+b_d=p} \binom{p}{b_1, b_2, \ldots, b_d} \prod_{j=i}^{d} x_j^{b_j}$$

ifadesine eşit olduğunu görürüz. Biraz karmaşık gözükebilir. Ancak endişelenmeye gerek yok çünkü modülo p'de baktığımızdan bazı terimler yok olacak. Bunun için katsayının p'ye bölünmesi yeterli. Biraz hesapla b_i'lerden herhangi biri p'ye eşit olmadığı sürece $\binom{p}{b_1,b_2,\ldots,b_d}$ sayısının her zaman p'ye bölündüğünü kolayca ispatlayabiliriz.

$$\binom{p}{b_1, b_2, \ldots, b_d} = \frac{p!}{b_1!b_2!\ldots b_d!}$$

eşitliği olduğuna göre ve bu ifade bir tamsayı olduğuna göre, şayet p bu ifadeyi bölmeseydi b_i'lerden en az birinin p'yi bölüp sadeleştirmiş olması gerekirdi. b_i'ler de p'den küçük sayılar olduğuna göre bu durum mümkün değil. Yani ancak b_i'lerden herhangi biri p'ye eşitse paydaki p sadeleşebilir ve geride p'ye bölünmez bir tamsayı kalır. Dolayısıyla ancak b_i'lerden birinin p'ye eşit olduğu terimler sıfırlanmıyor. O terimleri açıkça yazarsak

$$\sum_{j=1}^{d} x_j^p = \sum_{t\in({}^{\mathbb{Z}}/_{m\mathbb{Z}})^\times} \chi(t)\zeta_m^{pt} = \tau(\chi, p)$$

Gauss toplamına modülo p'de denk olduğunu görürüz. Öte yandan Gauss toplamları ile ilgili ispatladığımız ana teoremimize, yani Teorem 2'ye dayanarak $\tau(\chi, p) = \chi(p)\tau(\chi)$ diyebiliriz. Buradan da

$$\begin{aligned}\tau(\chi)^{p+1} &= [\tau(\chi)^2]^{\frac{p-1}{2}}\tau(\chi)^2 \\ &\equiv \chi(p)\tau(\chi)^2 \pmod p\end{aligned}$$

denkliği çıkar. Yine aynı teoremden $\tau(\chi)\tau(\overline{\chi}) = \tau(\chi)^2 = \chi(-1)m$ ve hipotezimizden $(\chi(-1)m, p) = 1$ olduğuna göre $\tau(\chi)^2$, modülo p'de tersinir diyebilir ve denklikten $\tau(\chi)^2$'yi sadeleştirerek

$$\left(\frac{\chi(-1)m}{p}\right) \equiv [\tau(\chi)^2]^{\frac{p-1}{2}} \equiv \chi(p) \pmod p$$

denkliğini elde edebiliriz. Göstermek istediğimiz de buydu.

Teorem 7. *p tek asal sayı olmak üzere*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8 \end{cases}$$

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & p \equiv 1 \textit{ veya } 3 \pmod 8 \\ -1, & p \equiv 5 \textit{ veya } 7 \pmod 8 \end{cases}$$

Kanıt. 6. teoremdeki fonksiyonel denklemi kullanmak istiyoruz. Dolayısıyla işimize gelecek şekilde bir $\chi \in X(8)$ ilkel kuadratik karakter tanımlayacağız :

$$\begin{aligned}\chi(a + 8\mathbb{Z}) &= (-1)^{\frac{(a-1)(a+1)}{8}} \\ &= \begin{cases} 1, & a \equiv \pm 1 \pmod 8 \\ -1, & a \equiv \pm 3 \pmod 8 \end{cases}\end{aligned}$$

olarak tanımlarsak tam da istediğimiz gibi bir χ elde etmiş oluruz. $\chi(-1) = 1$ olur.

$\left(\frac{2}{p}\right) = \left(\frac{2^3}{p}\right) = \left(\frac{8}{p}\right) = \left(\frac{\chi(-1)8}{p}\right)$ eşitliği geçerlidir. 6. iddiadaki fonksiyonel eşitliği de kullanırsak

$$\left(\frac{2}{p}\right) = \left(\frac{\chi(-1)8}{p}\right) = \chi(p) = (-1)^{\frac{(p-1)(p+1)}{8}}$$

olur. Euler kıstası ve Legendre sembolünün çarpımsal özelliği sayesinde de

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{2}{p}\right)$$

En sağdaki ifadenin teoremin beyanında belirtilen şartları sağladığı okur tarafından kolayca doğrulanabilir.

İkinci kuvvette karşılıklığı ispatlamaya hazırız.

Teorem 8. *(İkinci kuvvette Legendre sembolü karşılıklığı) p ve q farklı iki tek asal sayı olsun.*

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \\ &= \begin{cases} -1, & p \equiv q \equiv 3 \pmod 4 \\ 1, & \textit{diğer durumlarda} \end{cases}\end{aligned}$$

Kanıt. Hatırlıyoruz ki her q asal sayısının karakter grubunda, $(\mathbb{Z}/p\mathbb{Z})^\times$ döngüsel olduğundan, en az bir kuadratik karakter bulunmakta. Üreteç ω için $\chi_q(\omega^k) = (-1)^k$ karakterini tanımlamak bunu görmek için yeterli. Dolayısıyla 6. iddiadan

$$\begin{aligned}\left(\frac{p}{q}\right) &= \left(\frac{\chi_q(-1)q}{p}\right) \\ &= \left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right) \\ &= \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right)\left(\frac{q}{p}\right) \\ &= (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{q}{p}\right)\end{aligned}$$

İki tarafı da $\left(\frac{q}{p}\right)$ ile çarparsak

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \\ &= \begin{cases} -1 & p \equiv q \equiv 3 \pmod 4 \\ 1 & \text{diğer durumlarda} \end{cases}\end{aligned}$$

eşitliğini elde ederiz.

4 Neden Karşılıklık?

Tabii ki yazının başlığını ve teoremi gördükten sonra sorulacak en doğal soru bu. Neden karşılıklık? Kimle kim karşılıklı? Sayı teorisinin en temel ve önemli teoremlerinden biri olan karşılıklığın daha yüksek mertebelere genellenmesi başlı başına ileri matematiğin ilgi konularından biri. Öylesine bereketli bir teorem ki yüzlerce ispatı yayınlanmış ve genellikle sayı teorisinin Pisagor teoremi olarak anılıyor.

Aslında mesele modüler denklikleri çözmek. Lineer modüler denklikleri çözmeyi biliyoruz. $ax + b \equiv 0 \pmod m$ cinsinden bir denkliğin çözümünün varlığı tamamen a ve m sayılarının aralarında asal olup olmamasına bağlı. Varsa modülo m'de biricik çözümümüz $x = -ba^{-1}$ var. Eğer a tersinir değilse çözümümüz yok.

Ancak ikinci mertebeden denkliklere bakmaya başladığımız anda işler sarpa sarıyor. Bilindik cisimler $\mathbb{R}$ ve $\mathbb{C}$'de ikinci dereceden polinom kökü arar gibi, ya hiç kökü yoktur ya çakışık iki kökü vardır ya da ayrık iki kökü vardır diyemiyoruz. Misal $x^2 \equiv 1 \pmod 8$'in tam 4 tane çözümü var. 1, 3, 5 ve 7. Ancak Çin kalan teoremi sayesinde, herhangi bir modülo m bakmak yerine asallarda çözüm bakabildiğimiz için ve $\mathbb{Z}/p\mathbb{Z}$ de bir cisim olduğu için, yine sevdiğimiz sahalardayız ve 0,1 veya 2 çözümün varlığından bahsedebiliriz.

$ax^2 + bx + c \equiv 0 \pmod p$ gibi rastgele bir denkliğe bakarsak, $\mathbb{C}$ 'de ikinci dereceden bir polinom çözermişcesine $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ formülü uygulayamayız tabii ki. Çünkü herhangi bir cisimde kök nasıl alınır bilemiyoruz. Ki bu aslında çok derin bir soru.

İkinci dereceden ifadenin tamsayı katsayılı lineer ifadeler $(a_1x + b_1)(a_2x + b_2)$ biçiminde çarpanlara ayrılabilmesi de diğer bir durum. Burada da denkliği kolaylıkla çözebiliriz. Mesele iki tane lineer denkliği çözmekten ibaret. Bunu yapabileceğimizi de Çin kalan teoreminden biliyoruz. Eğer bu çarpanlara ayırma yöntemi de pek bariz değilse o zaman ne yapacağız? O zaman da ifadeyi tam kare haline getirme yöntemine başvuracağız. Denkliğin her iki tarafını $4a$ ile çarparsak

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod p$$

denkliğini elde ederiz. $b^2 - 4ac$'yi sağ tarafa atarsak

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod p$$

olur. Yani aslında mesele $y^2 \equiv m \pmod p$ cinsinden denklikleri çözmek.

Bu çözümleri anlamanın $\left(\frac{m}{p}\right)$ Legendre sembollerini anlamaktan geçtiğini, herhangi bir $m \in \mathbb{Z}$ için de $\left(\frac{m}{p}\right)$'yi anlamanın p'den farklı asal q için $\left(\frac{q}{p}\right)$'yi anlamaktan geçtiğini bu yazıda anlatmaya çalıştık. İkinci mertebeden karşılıklık bize $\left(\frac{q}{p}\right)$ Legendre sembolü ile $\left(\frac{p}{q}\right)$ Legendre sembolü arasındaki ilişkiyi söylüyor. Yani karşılıklı olan şeyler p ve q asalları. Zira $x^2 \equiv p \pmod q$ ve $x^2 \equiv q \pmod p$ denkliklerinin çözümlerinin herhangi bir ilişki içerisinde olduğu hiç de bariz değil.

Diyelim ki $\left(\frac{60}{89}\right)$ Legendre sembolünü hesaplamak, yani $x^2 \equiv 60 \pmod{89}$ denkliğinin bir çözümü var mı bilmek istiyoruz. $60 = 2^2 \cdot 3 \cdot 5$ olduğuna göre, $\left(\frac{2}{89}\right)^2\left(\frac{3}{89}\right)\left(\frac{5}{89}\right)$'i hesaplamalı. $89 \equiv 1 \pmod 8$ olduğuna göre Teorem 3.3.2'den $\left(\frac{2}{89}\right)^2 = 1$ çıktı. Kaldı elimizde $\left(\frac{3}{89}\right)\left(\frac{5}{89}\right)$. O zaman Teorem 6'nın 8. iddası *Legendre Karşılıklılığı*'nı kullanırsak $\left(\frac{3}{89}\right)$ ve $\left(\frac{5}{89}\right)$ ifadelerine takla attırabiliriz.

$$\begin{aligned}\left(\frac{3}{89}\right) &= (-1)^{\frac{3-1}{2}\frac{89-1}{2}}\left(\frac{89}{3}\right)\\ &= \left(\frac{89}{3}\right) = \left(\frac{2}{3}\right)\end{aligned}$$

ve

$$\begin{aligned}\left(\frac{5}{89}\right) &= (-1)^{\frac{5-1}{2}\frac{89-1}{2}}\left(\frac{89}{5}\right)\\ &= \left(\frac{89}{5}\right) = \left(\frac{4}{5}\right)\end{aligned}$$

modülo 3'de karelere bakmak kolay. 1'in karesi 1 ve 2'nin karesi $4 \equiv 1$ olduğuna göre, $\left(\frac{2}{3}\right) = -1$ olur. 4'ün modülo 5'de bir kare olduğunu hemen söylemek mümkün dolayısıyla

$$\left(\frac{60}{89}\right) = \left(\frac{2}{89}\right)^2\left(\frac{3}{89}\right)\left(\frac{5}{89}\right) = \left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = -1$$

yani $x^2 \equiv 60 \pmod{89}$ denkliğinin bir çözümü yok.

Bu yazıyı 119F405 numaralı "Temel Modüler Grupoid(TeMoG)" adlı Tübitak projesi bünyesinde hazırladık. Bu süreçte bize olan desteklerinden dolayı Tübitak'a teşekkürü borç biliriz.