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.

İkinci dereceden denklemler ele alındığında, yani $ax^2 + bx + c = 0$ şeklindeki tamsayı katsayılı deklemleri düşündüğümüzde, hepimizin aşina olduğu $\dfrac{-b \pm \sqrt{\Delta}}{2a}$ formülünün modülo m'de ifade edilmesi esnasında en büyük engelin karekök fonksiyonu olduğu hemen göze çarpar.

1 Modülo m'de n. kuvvetin kalanları

Bu kısımda temel kavramları tanımayı ve bazı yardımcı sonuçları ispatlamayı planlıyoruz. İlk olarak modüler aritmetikte kök alma kavramı ile başlayalım.

Tanım. n ve m iki pozitif tamsayı olsun. Bir a tamsayısı alalım. Eğer $a \equiv x^n \bmod m$ olacak şekilde bir x tamsayısı bulunabiliyorsa, a'ya modülo m'de bir n. kuvvetin kalanı diyelim.

Başka bir deyişle, verilen bir a tamsayısının m modunda n'inci kökünü alabiliyorsak a sayısına bir n'inci kuvvet kalanı diyeceğiz. Örneğin, 4 modunda tüm ikinci kuvvet (ya da kare) kalanları $\{0, 1\}$ kümesinden ibarettir. Yine modülo 4'te üçüncü kuvvet kalanları $\{0, 1, 3\}$ olmalıdır. Başka bir deyişle, modülo 4'te $\sqrt{0} = \{0, 2\}$ ve $\sqrt[3]{3} = 3$ olur.

Devam etmeden önce okuyucuya Çin Kalan Teoremi'ni bir hatırlatalım.

Teorem 1. *$\{m_1, m_2, \ldots, m_n\}$ kümesi ikişer olarak aralarında asal sayılardan oluşsun.*

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_n \bmod m_n \end{aligned}$$

denklem sisteminin modülo $M = m_1 \cdot m_2 \cdot \cdots \cdot m_n$ 'de biricik çözümü vardır.

Bu teoremi hatırladığımıza göre, Çin Kalan Teoremi'nin bu bağlamda nasıl işimize yaradığını ortaya koyan şu teoremi ispatlayabiliriz.

Teorem 2. *m ve n birden büyük birer tamsayı olsun. $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots p_r^{e_r}$, m'in asal çarpanlarına ayrılışı olduğunu varsayalım. O zaman,*

i. a tamsayısı modülo m'de bir n. kuvvetin kalanıdır ancak ve ancak her $i = 1, \ldots, r$ için a modülo $p_i^{e_i}$ 'de bir n. kuvvetin kalanıysa.

ii. p bir asal sayı olsun. $e \in \mathbb{N}$ olsun. a'yı, $d \in \mathbb{N}$ ve $p \nmid b$ olacak şekilde, $a = p^d b$ biçiminde yazalım. O halde a modülo p^e 'de bir n. kuvvetin kalanıdır ancak ve ancak

ya $d \geq e$ ise,

ya da $d < e$, $n \mid d$ ve b modülo p^{e-d} 'de bir n. kuvvetin kalanı ise.

Kanıt. Eğer $x^n \equiv a \bmod m$ ise $m \mid x^n - a$. Ama eğer $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots p_r^{e_r} \mid x^n - a$ ise her $i = 1, \ldots, r$ için $p_i^{e_i} \mid x^n - a$ olmalıdır. Dolayısıyla her $i = 1, \ldots, r$ için $x^n \equiv a \bmod p_i^{e_i}$ sağlanır.

Öte yandan her $i = 1, \ldots, r$ için $x_i^n \equiv a \bmod p_i^{e_i}$ denkliğini sağlayan bir $x_i \in \mathbb{Z}$ varsa, Çin Kalan Teoremi'ne göre

$$\begin{aligned} x &\equiv x_1 \bmod p_1^{e_1} \\ x &\equiv x_2 \bmod p_2^{e_2} \\ &\vdots \\ x &\equiv x_r \bmod p_r^{e_r} \end{aligned}$$

denklem sistemini sağlayan bir $x \in \mathbb{Z}$ vardır. O zaman elimizde

$$x^n \equiv x_i^n \equiv a \bmod p_i^{e_i}$$

$i = 1, \ldots, r$ eşitlikleri var. Öyleyse çözümün modülo m'deki biricikliğinden $x^n \equiv a \bmod m$ denkliğini elde ederiz.

İkinci iddiaya gelirsek eğer $d \geq e$ ise,

$$\begin{aligned} x^n \equiv a \bmod p^e &\Leftrightarrow x^n \equiv p^d b \bmod p^e \\ &\Leftrightarrow x^n \equiv 0 \bmod p^e \end{aligned}$$

olduğunu kolayca görürüz. $x = p^e$ seçmek yeterli.

Şimdi n'in d'yi böldüğünü varsayalım. O zaman $d = nk$ olacak şekilde bir $k \in \mathbb{Z}$ vardır. Öyleyse

$$\begin{aligned} b &\equiv x^n \bmod p^{e-d} \\ &\iff p^{e-d} | x^n - b \\ &\iff p^e | p^d (x^n - b) \\ &\iff p^e | p^{nk} x^n - p^d b \\ &\iff p^e | (xp^k)^n - a \end{aligned}$$

olmalıdır. xp^k'ya y dersek, a, y'nin modülo p^e'de $n.$ kuvvet kalanı olur.

Bir sayının $n.$ kuvvetin bir kalanı olduğunu görmek için asal kuvvetlere bakmanın yeterli olduğunu gördük. Şimdi asıl teoremimize gelebiliriz.

Teorem 3. *1. $p \nmid a$ olacak şekilde bir a tamsayısı alalım. a modülo p^e'de bir $n.$ kuvvet kalanı olsun. Tamsayı a'nın p^e modundaki $n.$ köklerinin kümesini A ile gösterelim, yani $A = \{x + p^e\mathbb{Z} \mid x^n \equiv a \bmod p^e\}$ şeklinde tanımlayalım. Eğer n sayısı çiftse d sayısı n'nin ikiye kaç kez kalansız bölündüğünü ifade etsin. O halde:*

$$\#A = \begin{cases} (n, p^e(p-1)) & p \neq 2 \text{ ise} \\ 1 & p = 2 \nmid n \text{ ise} \\ 2^{\min\{e-1, d+1\}} & p = 2 \\ & \text{ve } d \geq 1 \text{ ise} \end{cases}$$

2. Eğer p, n'i bölmüyorsa aşağıdaki önermeler denktir.

a modülo p^e'de bir $n.$ kuvvetin kalanıdır.

a modülo p'de bir $n.$ kuvvetin kalanıdır.

$$a^{\frac{p-1}{(p-1,n)}} \equiv 1 \bmod p$$

3. Bir $d \in \mathbb{N}$ için a modülo p^e'de bir p^d'inci kuvvetin kalanıysa aşağıdakiler geçerlidir:

$$p \neq 2 \text{ ise } a^{p-1} \equiv 1 \bmod p^{\min\{e, d+1\}}$$

$$p = 2 \text{ ise } a \equiv 1 \bmod 2^{\min\{e, d+2\}}$$

Uzun ve karmaşık görünen bu teoremde cebir imdadımıza yetişiyor. Birkaç önsav sayesinde teoremimizi kolay bir şekilde ispatlayabileceğiz.

Önsav 1. *$p \neq 2$ ise, $(\mathbb{Z}/p^e\mathbb{Z})^\times$, $p^{e-1}(p-1)$ elemanlı döngüsel bir gruptur ve $\{x + p^e\mathbb{Z} | x \equiv 1 \bmod p\}$ kümesi bu grubun p^{e-1} elemanlı bir altgrubunu teşkil eder. Bu altgrup $(1+p) + p^e\mathbb{Z}$ tarafından üretilir.*

Kanıt. $(\mathbb{Z}/p^e\mathbb{Z})^\times$ grubundaki elemanlar $0 < x < p^e$ şeklinde p^e ile aralarında asal olan x tamsayılarıdır. Bu aralıktaki herhangi bir x için x ve p^e'nin en büyük ortak bölenleri p^d,$0 < e$ biçiminde bir sayı olmalı. Dolayısıyla bu aralıkta p^e ile aralarında asal olmayan sayılar, sırayla yazılması gerekirse, $p, 2p, 3p, \ldots, p^{e-1} \cdot p$ sayılarıdır. Bunlardan p^{e-1} tane var (sondaki $p^{e-1} \cdot p$ ile 0'ı kastettiğimizi belirtelim). $\mathbb{Z}/p^e\mathbb{Z}$'nin de p^e tane elemanı olduğuna göre, $(\mathbb{Z}/p^e\mathbb{Z})^\times$'de $p^e - p^{e-1} = p^{e-1}(p-1)$ tane eleman var. $\{x + p^e\mathbb{Z} | x \equiv 1 \bmod p\}$ altgrubunun da eleman sayısını sayalım. $1 + p, 1 + 2p, \ldots, 1 + p^{e-1} \cdot p$ bu altgrubun modülo p'de 1'e denk olaman elemanları. Sonuncu elemanla 1'i kastediyoruz. Burada da görüyoruz ki p^{e-1} tane eleman var. $1 + p$ elemanının mertebesinin de p^{e-1} olduğunu söyleyebilirsek, bu altgrubu ürettiğini göstermiş oluruz. Yani yapmamız gereken şey,

$$(1+p)^{p^{e-1}} \equiv 1 \ mod\ p^e$$

denkliğini ispatlamak. Onun için de şu denkliğe başvuracağız:

$$(1+p)^{p^e} \equiv 1 + p^{e+1} \ mod\ p^{e+2}$$

$e = 0$ için aşikâr. $e = 1$ için $(1+p)^p \equiv 1 + p^2 \ mod\ p^3$ denkliğini görmek için $(1+p)^p$'yi binom yasasıyla açalım.

$$(1+p)^p = 1 + p \cdot p + \binom{p}{2} p^2 + \cdots + p \cdot p^{p-1} + p^p$$

İlk iki terim hariç hepsinin p^3 sayısına bölüneceğini hemen görebiliyoruz. Dolayısıyla denklik geçerli. Şimdi denkliğin $e-1$ için de geçerli olduğunu varsayalım. $u \in \mathbb{Z}$ için,

$$(1+p)^{p^e} = ((1+p)^{p^{e-1}})^p \equiv (1 + p^e + u \cdot p^{e+1})^p$$

geçerli olacaktır. Neyseki en sondaki ifadeyi açıkça yazmayı biliyoruz.

$$\sum_{a_1+a_2+a_3=p} \binom{p}{a_1, a_2, a_3} 1^{a_1} (p^e)^{a_2} (up^{e+1})^{a_3}$$

Şimdi terimleri inceleyelim. $a_2 \geq 2$ ise $(p^e)^{a_2}$'li terim için, $e > 1$ olduğundan, $a_2 \cdot e \geq 2e \geq e + 2$ eşitsizlikleri geçerli. Dolayısıyla bu terimler modülo

p^{e+2}'de sadeleştiler. Aynı şekilde $a_3 \geq 2$ için $a_3 \cdot (e+1) \geq 2e+2 \geq e+2$. Dolayısıyla o terimler de sadeleşti. $a_2 = a_3 = 1$ için gelen terim de $u \cdot p^{2e+1}$ olduğundan gitti.

$(a_2, a_3) = (1,0), (0,1), (0,0)$ durumları kaldı. $(1,0)$ olduğunda $a_1 = p-1$ olacak ve dolayısıyla multinom katsayısı p gelecek Buradan $p \cdot p^e = p^{e+1}$'li sadeleşmeyen bir terim elde edeceğiz. $(0,1)$ olduğunda yine p multinom katsayısı gelecek ancak terim $p \cdot up^{e+1}$ olduğundan sadeleşecek. $(0,0)$'dan da yalnızca 1 geliyor. Dolayısıyla elimizde yalnızca $1 + p^{e+1}$ kaldı. Göstermek istediğimiz de buydu.

İspatladığımız denklikte e yerine $e-1$ yazarsak $(1+p)^{p^{e-1}} \equiv 1+p^e \ mod\ p^{e+1}$ denkliğini elde ederiz. Buradan da $(1+p)^{p^{e-1}} \equiv 1 \ mod\ p^e$ çıkar.

Önsav 2. *$e \geq 2$ ise*

$$U = \{x + 2^e\mathbb{Z} | x \equiv 1 \mod 4\}$$

kümesi 2^{e-2} elemanlı bir döngüsel gruptur, dahası $5 + 2^e$ tarafından üretilir, yani $U = \langle 5 + 2^e\mathbb{Z} \rangle$.

Kanıt. Bu grup $5 = 1 + 1 \cdot 4, 1 + 2 \cdot 4, 1 + 3 \cdot 4, \ldots, 1 + 2^{e-3} \cdot 4, 1 + 2^{e-2} \cdot 4 = 1$ elemanlarından oluştuğuna göre 2^{e-2} elemanı var. Şimdi

$$5^{2^{e-2}} \equiv 1 \ mod\ 2^e$$

denkliğini göstermeli. Bir önceki önsava benzer bir şekilde

$$5^{2^k} \equiv 1 + 2^{k+2} \ mod\ 2^{k+3}$$

denkliğini kullanacağız. $k = 0$ durumu yine bariz. $k = 1$ durumu da ufak bir hesapla doğrulanabilir. $k-1$ için denkliğimiz geçerliyse

$$5^{2^k} = (5^{2^{k-1}})^2 \equiv (1 + 2^{k+1} + u2^{k+2})^2 \ mod\ 2^{k+3}$$

En sondaki ifadeyi açarsak

$$1+(2^{k+1})^2+(u2^{k+2})^2+2(2^{k+1}+u2^{k+2}+2^{k+1}u2^{k+2})$$

elde ederiz. Gerekli sadeleştirmeleri yaptıktan sonra elimizde yalnızca $1 + 2^{k+2}$ kalır. Bu sefer de $k = e-2$ yazarak hedeflediğimiz denkliği elde ederiz.

Önsav 3. *G, birim elemanı 1 ile gösterilen n elemanlı bir döngüsel grup olsun. G'deki bir eleman a'nın d. kuvvet olması $a^{\frac{n}{(n,d)}} = 1$ eşitliğini sağlamasına denktir. Eşitliğin geçerli olduğu durumda da d. kuvveti a olan elemanların sayısı (n,d) tanedir.*

Kanıt. Bir $x \in G$ için $x^d = a$ olduğunu varsayalım. O halde

$$a^{\frac{n}{(n,d)}} = (x^d)^{\frac{n}{(n,d)}} = (x^n)^{\frac{d}{(n,d)}} = 1$$

Şimdi $a^{\frac{n}{(n,d)}} = 1$ olduğunu varsayalım. Döngüsel grubumuzu $g \in G$ üretiyor olsun. Öyleyse bir $t < n$ doğal sayısı için $g^t = a$ olmalı. Yani elde $a^{\frac{n}{(n,d)}} = (g^t)^{\frac{n}{(n,d)}} = 1$ eşitliği var. Grubun da mertebesi n olduğuna göre, $n \mid \frac{tn}{(n,d)}$ olmalı. Öyleyse (n,d) sayısı t'yi bölmeli. O zaman Bézout teoremine göre $xn+yd = t$ olacak şekilde iki tane x, y tamsayısı var. Bu durumda $a = g^t = g^{xn+yd} = g^{xn}g^{yd} = (g^y)^d$. Yani a bir d. kuvvet oldu.

Kanıt (Teoremin kanıtı)**.** Şimdi, $p \neq 2$ iken Önsav 1 sayesinde $(\mathbb{Z}/p^e\mathbb{Z})^\times$'in döngüsel olduğunu söyleyebiliriz. Böylelikle Önsav 3'ü de kullanarak İddia 1'i göstermiş oluruz. 2. iddia için, yine Önsav 3'ye dayanarak, eğer a modülo p^e'de bir n. kuvvet kalanıysa ve

$$B = \frac{\#(\mathbb{Z}/p^e\mathbb{Z})^\times}{(\#(\mathbb{Z}/p^e\mathbb{Z})^\times, n)}$$

olarak belirlersek $a^B \equiv 1 \mod p^e$ olur. Eğer p, n'i bölmüyorsa $(p^{e-1}(p-1), n) = (p-1, n)$ olur. Eğer x bir tamsayı ise yine A şıkkında tespit ettiğimiz p^{e-1} mertebeli altgruba dayanarak $x^{p^{e-1}} \equiv 1 \mod p^e \Leftrightarrow x \equiv 1 \mod p$ denkliğinin geçerliliğini doğrulayabiliriz. O zaman,

$$a^B = (a^{\frac{p-1}{(p-1,n)}})^{p^{e-1}} \equiv 1 \bmod p^e$$
$$\Leftrightarrow a^{\frac{p-1}{(p-1,n)}} \equiv 1 \bmod p$$

olmuş oluyor. Bu da teoremin ikinci iddiasının $p \neq 2$ için doğru olduğunu gösteriyor. 3. iddiayı kanıtlayalım. Eğer $n = p^d$ cinsinden ise

$$k = e - 1 - \min\{d, e-1\}$$

olmak şartıyla, yukarıda belirlediğimiz B sayısı $B = p^k(p-1)$ olmalı. İspatladığımız 2. iddianın üçüncü önermesine göre

$$a^{\frac{p-1}{(p-1,p^d)}} = a^{p-1} \equiv 1 \mod p$$

olduğuna göre a sayısı A'daki altgruba ait olmalı. Bu altgrup $(1+p) + p^e\mathbb{Z}$ tarafından üretiliyordu. Dolayısıyla bir $l \in \{0, 1, \ldots, p^{e-1}-1\}$ sayısı için

$$a^{p-1} \equiv (1+p)^l \mod p^e$$

olmalı. O zaman

$$\begin{aligned} a^B &= (a^{p-1})^{p^k} \\ &\equiv ((1+p)^l)^{p^k} = (1+p)^{lp^k} \bmod p^e \end{aligned}$$

denkliği geçerli. Yani $a^B \equiv 1 \bmod p^e$ ise

$$(1+p)^{lp^k} \equiv 1 \bmod p^e$$

olmalı. $(1+p) + p^e\mathbb{Z}$'nin mertebesi p^{e-1} olduğuna göre, lp^k mertebeye bölünmeli yani $p^{e-1} \mid$

lp^k olmalı. Her iki taraftan p^k sadeleştirilirse $p^{\min\{d,e-1\}} \mid l$ olması gerektiği görülür. O zaman da

$$(1+p)^l \equiv 1 \bmod p^{\min\{d,e-1\}+1}$$

vardır. $(1+p)^l$ yerine tekrar a^{p-1} yazarsak

$$a^{p-1} \equiv 1 \bmod p^{\min\{d+1,e\}}$$

elde ederiz. Ki bu da tam olarak göstermek istediğimiz şeydi. Yukarıdaki son argümanları özetlemek gerekirse,

$$\begin{aligned} a^B \equiv 1 \mod p^e \\ &\Leftrightarrow (1+p)^{lp^k} \equiv 1 \bmod p^e \\ &\Leftrightarrow p^{e-1} \mid lp^k \\ &\Leftrightarrow p^{\min\{d,e-1\}} \mid l \\ &\Leftrightarrow (1+p)^l \equiv 1 \bmod p^{\min\{d,e-1\}+1} \\ &\Leftrightarrow a^{p-1} \equiv 1 \bmod p^{\min\{d+1,e\}} \end{aligned}$$

Şimdi $p = 2$ durumuna geçelim. Eğer $2 \nmid n$ ise $x \to x^n$ fonksiyonu $(\mathbb{Z}/p^e\mathbb{Z})^\times$'in bir otomorfisi olacak. Endomorfisi olduğunu görmek kolay. Çekirdeğini incelemek gerekirse $x^n = 1$ olabilmesi için, $(\mathbb{Z}/p^e\mathbb{Z})^\times$'de mertebesi n'yi bölen bir eleman x olmalı. Ama bu x'in mertebesi aynı zamanda grubun mertebesi 2^{e-1}'i bölmeli. Bu durumda x'in mertebesi için olası değerler $0 < t < e-1$ olması kaydıyla 2^t veya 1. 2^t olamaz çünkü hipotezimiz gereği n tek. Dolayısıyla x'in mertebesi 1. Dolayısıyla $x = 1$. Yani çekirdek 1'den ibaret. Sonlu bir grubun birebir endomorfisi aynı zamanda örten olacağına göre, $x \to x^n$ bir otomorfiymiş. O halde $x^n \equiv a \bmod 2^e$ ancak bir eleman tarafından sağlanabilir. 1. iddianın ikinci durumu ispatlandı.

Şimdi $n = 2^d u$ cinsinden olduğunu varsayalım. Tabii ki $d \geq 1$ ve $2 \nmid u$ olsun. $e = 1, 2$ için 1. iddianın geçerliliği aşikar. Dolayısıyla $n \geq 3$ için inceleyelim. Önsav 2'den

$$\#\{x + 2^e\mathbb{Z} \mid \ x \equiv 1 \mod 4\} = 2^{e-2}$$

ve ardından Önsav 3'ten de

$$\begin{aligned} \#\{x + 2^e\mathbb{Z} \mid \ x^n \equiv a \mod 2^e\} &= (2^{e-2}, 2^d) \\ &= 2^{\min\{d,e-2\}} \end{aligned}$$

eşitliklerini elde ederiz.

O zaman $\{x + 2^e\mathbb{Z} |\ x^n \equiv a \bmod 2^e\}$ kümesinin

$$\{x + 2^e\mathbb{Z} |\ x^n \equiv a \bmod 2^e \ \&\ x \equiv 1 \mod 4\}$$

kümesi ve

$$\{-x + 2^e\mathbb{Z} |\ x^n \equiv a \bmod 2^e \ \&\ x \equiv 1 \mod 4\}$$

kümesinin ayrık birleşimi olduğunu da göz önünde bulundurunca

$$\begin{aligned} \#\{x + 2^e\mathbb{Z} |\ x^n \equiv a \mod 2^e\} &= 2 \cdot 2^{\min\{d,e-2\}} \\ &= 2^{\min\{d+1,e-1\}} \end{aligned}$$

eşitliğini elde edebiliriz. Böylelikle ilk iddianın ispatı tamamlanmış oldu. Üçüncü iddiaya gelelim. Eğer $e \geq 2$ ve a modülo 2^e 'de bir 2^d. kuvetin kalanıysa $a \equiv 1 \bmod 4$ olur. O zaman $a \in U$. Öyleyse bir $l \in \{0, 1, \ldots, 2^{e-2} - 1\}$ için

$$5^l \equiv a \bmod 2^e$$

eşitliği olmalı. Ve tekrar Önsav 2'e dayanarak

$$\begin{aligned} B = \frac{\#U}{(\#U, n)} = \frac{2^{e-2}}{(2^{e-2}, 2^d u)} \\ = 2^{e-2-\min\{e-2,d\}} \end{aligned}$$

Eğer $k = 2^{e-2-\min\{e-2,d\}}$ yazarsak

$$a^B \equiv 5^{2^k l} \bmod 2^e$$

denkliğini elde ederiz. O zaman,

$$\begin{aligned} a^B \equiv 1 \bmod 2^e \\ &\Leftrightarrow 2^{e-2} \nmid 2^k l \\ &\Leftrightarrow 2^{\min\{d,e-2\}} \mid l \\ &\Leftrightarrow 5^l \equiv 1 \bmod 2^{\min\{d,e-2\}+2} \\ &\Leftrightarrow a \equiv 1 \bmod 2^{\min\{d,e-2\}+2} \end{aligned}$$

Üçüncü iddia da kanıtlanmış oldu.

Nihayet yazımızın ana teoremini sunacağımız bölüme geldik. Buraya kadar yapmış olduğumuz hazırlık bize karşılıklılık teoremini ispatlamada yardımcı olacak. İlk olarak Legendre sembolünü tanımlayalım.

Tanım. p tek bir asal sayı olsun. $a \in \mathbb{Z}$ tamsayısı p'nin bir katı olmasın. O zaman a ve p sayılarının *Legendre sembolü* $\left(\frac{a}{p}\right)$'yi, eğer a modülo p'de bir ikinci kuvvet kalanıysa $\left(\frac{a}{p}\right) = 1$ değilse $\left(\frac{a}{p}\right) = -1$ olacak şekilde tanımlayalım.

Görüldüğü üzere a tamsayısının Legendre sembolü tamamen a'nın modülo p'deki kalan sınıfına bağlı. Çünkü a'nın kalan sınıfı α eğer modülo p'deki kalan sınıflarının birinin karesine eşitse $\left(\frac{a}{p}\right) = \left(\frac{\alpha}{p}\right) = 1$, değilse $\left(\frac{a}{p}\right) = \left(\frac{\alpha}{p}\right) = -1$ olacak.

$(\mathbb{Z}/p\mathbb{Z})^\times$'ın döngüsel bir grup olduğundan bahsetmiştik. ω bir üreteç olsun. Herhangi bir $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ için $a = \omega^k$ olacak şekilde bir k tamsayısı olduğundan,

$$\left(\frac{a}{p}\right) = \left(\frac{\omega^k}{p}\right)$$

eşitliğini elde ederiz. Peki ω üretecinin Legendre sembolü 1 olabilir mi? Eğer 1 olsaydı bu karesi ω olan bir $t \in (\mathbb{Z}/p\mathbb{Z})^\times$ elemanının varlığını gerektirirdi. Ancak bir üreteç kendi karekökünü nasıl üretebilir? Bu tezatlıktan kurtulmak için $\left(\frac{\omega^k}{p}\right) = (-1)^k$ olmalı. Bu eşitlik $a \mapsto (\frac{a}{p})$ eşleşmesinin $(\mathbb{Z}/p\mathbb{Z})^\times$ ve $\{\pm 1\}$ arasında bir homomorfizma olduğunu, diğer bir değişle $(\frac{\cdot}{p})$ fonksiyonunun bir modülo p kuadratik karakteri olduğunu söylüyor. Bu sayede gönül rahatlığıyla Legendre sembolünün çarpımsal olduğunu söyleyebiliriz. Dahası her modülo p karakterini Dirichlet karakteri olarak tüm $\mathbb{Z}$'ye genişletebildiğimize göre, her $a \in p\mathbb{Z}$ için $(\frac{a}{p}) = 0$ diyebiliriz. Şimdi önceki bölümlerde yaptıklarımızın meyvelerini toplayalım.

Teorem 4. *(Euler Kıstası) Bir p tek asal sayısı ve a tamsayısı için*

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

Kanıt. Verilen a tamsayısının p'nin katı olduğu durumda iddia edilen denkliğin sağlandığı kolayca görülebilir. Öyleyse $a \notin p\mathbb{Z}$ varsayabiliriz. Teorem 3'e göre:

$$\begin{aligned}\left(\frac{a}{p}\right) = 1 \Leftrightarrow \exists x \in \mathbb{Z}, a \equiv x^2 \quad & \mod p \\ \Leftrightarrow a^{\frac{p-1}{(p-1,2)}} = a^{\frac{p-1}{2}} \equiv 1 \quad & \mod p\end{aligned}$$

ki bu da gösterilmek istenen iddia idi.

Ana teoremimizi sunmaya hazırız:

Teorem 5. *1. 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.

2. p tek asal sayı olmak üzere

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

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

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

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

Kanıt. 1. 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.

$$\tau(\chi)^p = \left(\sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(t)\zeta_m^t\right)^p.$$

Bu noktada multinom açılımı imdadımıza yetişiyor. Multinom açılımı aslında Önsav 2'de kullandığımız açılımın bir genellemesi. 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 isimli yazıda ispatladığımız **Teorem X**'e dayanarak $\tau(\chi,p) = \chi(p)\tau(\chi)$ diyebiliriz. Buradan da

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

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

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

denkliğini elde edebiliriz. Göstermek istediğimiz de buydu.

2. 1. iddiadaki fonksiyonel denklemi kullanmak istiyoruz. Dolayısıyla işimize gelecek şekilde bir $\chi \in X(8)$ ilkel kuadratik karakter tanımlayacağız:

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

olarak tanımlarsak tam da istediğimiz gibi bir χ elde etmiş oluruz. $\chi(-1) = 1$ olur. Teorem 3'ün 2. iddiasına göre $\left(\frac{2}{p}\right) = \left(\frac{2^3}{p}\right) = \left(\frac{8}{p}\right) = \left(\frac{\chi(-1)8}{p}\right)$ eşitliği geçerlidir. 1. 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.

3. Her q asal sayısının karakter grubunda, $(\mathbb{Z}/p\mathbb{Z})^\times$ döngüsel olduğundan, en az bir kuadratik karakter bulunduğunu hatırlıyoruz. Üreteç ω için $\chi_q(\omega^k) = (-1)^k$ karakterini tanımlamak bunu görmek için yeterli. Dolayısıyla 1. 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

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

eşitliğini elde ederiz.

2 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. $ax + b \equiv 0 \bmod m$ 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 $x^2 \equiv 1 \bmod 8$'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.

$ax^2+bx+c \equiv 0 \bmod p$ 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

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

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

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

olur. Yani aslında mesele $y^2 \equiv m \bmod p$ 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 $x^2 \equiv p \bmod q$ ve $x^2 \equiv q \bmod p$ denkliklerinin çözümlerinin herhangi bir ilişki içerisinde olduğu hiç de bariz değil.

Diyelim ki $\left(\frac{60}{89}\right)$ Legendre sembolünü hesaplamak, yani $x^2 \equiv 60 \bmod 89$ 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. $89 \equiv 1 \bmod 8$ olduğuna göre Teorem 5.2'den $\left(\frac{2}{89}\right)^2 = 1$ çıktı. Kaldı elimizde $\left(\frac{3}{89}\right) \left(\frac{5}{89}\right)$. O zaman Teorem 5'nın 3. 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'te 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 $x^2 \equiv 60 \bmod 89$ 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