Proje Raporu

Kalan Sınıfları Üzerinde Olasılık Hesabı

İçindekiler

1. GİRİŞ

Bu bölümde ele alınan problem durumu, araştırmanın amacı ve sınırlılıkları ifade edilmiştir.

1.1. Problem Durumu

Matematikte kimi zaman bir konunun daha önce uygulanmadığı yeni sahalar üzerine uygulanması da değerli olabilmektedir. Bu proje, bu türden bir uygulamayı içermektedir. Bu çalışmada, olasılığın modüler aritmetik konu alanına bir uygulanışı çalışılmıştır.Hem olasılığın, hem de modüler aritmetiğin fikri kökenleri çok eskilere dayansa da formel gelişimleri matematik tarihinde nispeten yeni sayılabilir.

Bugünkü anlamıyla istatistik ve olasılığın konusu başlıca; şans oyunları, insan hayatı ve ölçümlerine ilişkin biriken kayıtlardan kaynaklanır. Bu kaynakların her ikisi de, gerçekten tanımlanabilir biçimde, on yedinci yüzyılın ortalarından itibaren ortaya çıkar. Klasik olasılık kavramı, bu kaynakların ilkinden, deneysel olasılık kavramı ise istatistikler üzerine kurulu ikinci kaynağa bağlı olarak gelişmiştir. 1650 yıllarında kumar Fransız toplumunda çok yaygındı. Zar, kart, para atışı, rulet gibi oyunlar oldukça gelişmişti. Paraya olan ihtiyacın artması bazı formüllerle kumar şansının hesaplanabileceği düşüncesini getirdi. Méré gibi etkili, sözü geçen kumarbazlar Pascal, Fermat ve daha sonra d'Alembert ve De Moivre gibi zamanın önde gelen matematikçilerinin bu konuda yardımcı olabileceğini düşündüler. Matematikçilerin problemi benimsemesiyle klasik olasılık konusu şekillendi. Olasılığın (prior) tanımı 1654 yılında Pascal ve Fermat arasındakiyazışmalarda formüle edildi. Huygens 1657 yılında konuyla ilgili ilkbilimsel eseri yayınladı (URL-1).Modüler aritmetik ise ilk olarak Carl FriedrichGauss'un 1801 yılında yayınlanan "DisquisitionesArithmeticae" isimli kitabında tanıtılmıştır (URL-2).Modüler aritmetik, saat-gün gibi zamanla ilgili somut problemlerden yola çıkarak bir tamsayı yerine onun kalanı üzerinden temsilini denklik ile gösteren bir aritmetiği içermektedir. Gerek olasılık gerekse de modüler aritmetik günlük hayatta karşılığı çok fazla olan ve pek çok uygulama alanları bulunan konular olarak gelişmeye ve uygulama alanlarına taşınmaya devam etmektedir.

Bu çalışmada da olasılık ile modüler aritmetik arasında kalan sınıfları üzerinden yeni bir ilişkilendirmekurulmak istenmiştir.Bu yaklaşım çerçevesinde, modüler aritmetiğe konu olan çeşitli kavram ve uygulamalar üzerinde çeşitli olasılık incelemeleri ve hesaplamaları yapılmaya çalışılmıştır.

Bu çalışmada üretilen ilişkilendirmenin daha sonra bu alanla da bağlantıları kurulabilecek bazı olasılık problemleri için özellikle sonsuz elemanlı ayrık sayı kümelerinin olasılık hesaplamalarına yönelik bir katkı sağlaması umulmaktadır.

1.2. Araştırmanın Amacı

Bu çalışmada, olasılık teorisinin sonsuz kümelerden oluşan tamsayıların kalan sınıflarına uygulanışını incelemek amaçlanmıştır. Bu amaç, doğrultusunda uygulama alanları belirlenmiş ve uygulama örnekleri üretilmiştir.

1.3. Sınırlılıklar

Bu çalışmanın uygulama alanları bu çalışmanın sınırlılıklarını ortaya koymaktadır. Bu çalışma aşağıdaki uygulama alanları ile sınırlandırılmıştır.

- Kalan sınıfları ile ilgili birleşim, kesişim olaylarının olasılığı
- Modüler aritmetikte kare kalan, küp kalan ve daha yüksek kuvvetlerden kalanlar ile ilgili olasılık hesaplaması
- Kalan sınıfları ile şartlı (koşullu) olasılık uygulaması

- Fermat'ın Küçük Teoremi ileolasılıkuygulaması
- Euler'in φ fonksiyonu ileolasılık uygulaması
- Modüler aritmetik probleminde olasılık hesaplanması

2. YÖNTEM

Bu bölümde, bu çalışmanın üzerine inşa edildiği matematiksel alt yapı ve geliştirilen uygulamanın teorik alt yapısı tanıtılmıştır.

2.1. Uygulamanın Dayandırıldığı Matematiksel Alt Yapı

Uygulama sırasında kullanılan kalan sınıfları, modüler aritmetik ve olasılıkla ilgili kavramlar şunlardır.

Kalan sınıfları: Tamsayıların n ile bölünerek verdiği kalana göre sınıflandırılmasıyla oluşan sayı kümelerini ifade eder. Z/n şeklinde gösterilir. Z/n tamsayıların n ile bölümünden oluşan kalan sınıflarını ifade eder.

Z/n = $\{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1},\}$ sınıflarından oluşur. Bu sınıfların her biri sonsuz elemanlıdır. Aşağıda bu sınıfların her birine giren tamsayılar gösterilmiştir.

$\overline{0} = \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots, k.n, \dots\}$(3 ile bölündüğünde 0 kalanını veren tamsayılar)

$\overline{1} = \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, 3n+1, \dots, kn+1, \dots\}$(n ile bölündüğünde 1 kalanını veren tamsayılar)

$\overline{2} = \{\dots, -2n+2, -n+2, 2, n+2, 2n+2, kn+2, \dots\}$(n ile bölündüğünde 2 kalanını veren tamsayılar)

...

$\overline{n-1}$= $\{\dots -1, n-1, 2n-1, 3n-1, \dots\}$(n ile bölündüğünde n-1 kalanını veren tamsayılar.

Bu n tane kalan sınıfın her biri ikişer ikişer ayrıktır.

Modüler Aritmetik: Bir tamsayı yerine o tamsayıya denk olan(aynı kalan sınıf içine giren)tamsayılarla gerçekleştirilen aritmetik işlemlerdir.

Denklik: a ve b tamsayılarının sıfırdan farklı aynı m tamsayısı ile bölümünden elde edilen kalanlar eşit ise a ve b tamsayılarına (mod m) de birbirlerine denktir denir. a ≡ b (mod m) şeklinde gösterilir. a ≡ b (mod m) ↔ $a - b = m.k\ (k \in Z)$

Kuvvet Kalan: Bir tamsayının herhangi bir pozitif tamsayı kuvvetinin 1'den büyük belirli bir doğal sayı ile bölümünden kalanı gösterir. Bu işlem tamsayının karesi alınarak yapılırsa kare kalan, küp alınarak yapılırsa küp kalan adını alır.

$a^2 \equiv x\ (mod\ m)$kare kalan x'tir. $a^3 \equiv y\ (mod\ m)$küp kalan y'dir.

Fermat'ın Küçük Teoremi: p bir asal sayı ve a∈ Z^+ ile p aralarında asal olmak üzere $a^{p-1} \equiv 1\ (modp)$'dir.

Euler'in$\boldsymbol{\varphi}$ fonksiyonu: Bu fonksiyon tanımlanırken aşağıdaki kavramlar aracılığıyla tanımlanmaktadır.

$\boldsymbol{\varphi(n)} = \{\boldsymbol{n'den}$ küçü$\boldsymbol{k\ ve\ n\ ile\ aralarında\ asal\ olan\ pozitif\ tamsayıların\ sayısı}\}$

n sayısının asal bölenleri $\alpha_1, \alpha_2, \dots, \alpha_k$ olmak üzere,

$$\boldsymbol{\varphi(n) = n.\left(1 - \frac{1}{\alpha_1}\right).\left(1 - \frac{1}{\alpha_2}\right)...(1 - \frac{1}{\alpha_k})}$$

a ile n aralarında asal olmak üzere,

$a^{\boldsymbol{\varphi(n)}} \equiv 1\ (mod(n))$ bağıntısı bulunmaktadır.

Olasılık Kavramları: Bu çalışmada olasılık hesaba ilişkin şu kavramlar kullanılmıştır.

Örnek Uzay: Rassal bir deneyde mümkün olan tüm çıktıları gösteren kümedir. "E" ile gösterilir.

Örnek uzay, içerdiği eleman sayısı açısından iki sınıfa ayrılır: a) Sayılabilir (sonlu/sonsuz) elemanlı b) Sayılamaz (sonsuz) elemanlı Eğer bir örnek uzayın elemanları, tam sayıların bir alt kümesi ile birebir ilişkili ise örnek uzay sayılabilir elemanlıdır. Ayrıca bir örnek uzayı sonlu sayıda elemana sahip ise sayılabilirdir. Sayılamayacak kadar çok (sonsuz) elemana sahip kümeler için verilebilecek örnek, tüm gerçel sayıların tanımlandığı kümedir. Reel sayıları saymak mümkün değildir (URL-3).

Olay: Örnek uzayın herhangi bir alt kümesine verilen isimdir.

Bir olayın olasılığı: Herhangi bir olayın gerçekleşme olasılığını ifade eder. P ile gösterilir. P(A) bir A olayının olasılığını gösterir. s(A), A kümesinin ve s(E) örnek uzayın eleman sayısını göstermek üzere, bir A olayının olasılığı Bağıntı-1'de gösterilen biçimde hesaplanır.

$$p(A) = s(A)/s(E)$$

Bağıntı-1

Kesişim Olayının Olasılığı: Aynı örnek uzayda yer alan iki olayın kesişim olayının olasılığı, Bağıntı-2'de gösterildiği biçimde hesaplanır.

$$p(A \cap B) = s(A \cap B)/s(E)$$

Bağıntı-2

Birleşim Olayının Olasılığı: Aynı örnek uzayda A ve B gibi iki olay için A veya B'nin gerçekleşme olasılığına A ve B olaylarının birleşim olayının olasılığı denir. Bu olasılık $P(A \cup B)$ ile gösterilir ve Bağıntı-3'te gösterildiği biçimde hesaplanır.

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Bağıntı-3

Koşullu Olasılık: Bir olayın gerçekleşme şartına bağlı olarak ikinci bir olayın gerçekleşme olasılığıdır. Aynı örnek uzaya ait A ve B olayları göz önüne alınsın; B olayının gerçekleşmiş olduğu bilindiğine göre A olayının gerçekleşme olasılığı P(AIB) ile gösterilir ve Bağıntı-4'te gösterildiği biçimde hesaplanır.

$$P(AIB) = P(A \cap B)/P(B)$$

Bağıntı-4

2.2. Uygulamanın Dayandırıldığı Teorik Alt Yapı

Bilindiği üzere, tam sayılar kalan sınıflarına ayrılabilmektedir. Bu durum için kullanılan gösterilişlerden biri Z/n gösterimidir. Z/nkümesinin içerdiği kalan sınıfları da

$Z/n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}, \}$biçiminde ifade edilebilir.

Bu kümedeki her bir kalan sınıf sonsuz elemanlıdır. Bir tamsayının n ile bölümünden kalanına göre bu tamsayı ilgili kalan sınıfa yerleştirilmektedir. Bu çalışmada, Aksiyom-1 ile sunulan varsayıma dayalı olarak olasılığın yeni bir uygulama biçimi geliştirilmiştir.

Aksiyom-1: Tamsayılar Z/n biçiminde kalan sınıflarına (kalan sınıfları sonsuz elemanlı olacak biçimde) ayrıldığında seçilen her bir tamsayının bu kalan sınıflardan birinde olma olasılığı eşittir.

Aksiyom-1 çerçevesinde, Z/n kümesini olasılık konusundaki eş olumlu ve n elemanlı bir örnek uzaya benzetebiliriz. Bu durumda, her bir kalan sınıf da bu örnek uzayın bir çıktısını gösterir. Her kalan sınıf eş olumlu bir örnek uzaya ait bir çıktıyı gösterdiğinden seçilen herhangi bir tamsayının belli bir kalan sınıfa ait olma olasılığı 1/n olur. Aksiyom-1'e dayalı olarak ortaya konan bu gözlem, bu projedeki olasılık uygulamalarının da temelini oluşturmuştur. Bu varsayımdan hareketle, bu çalışmanın bulgular bölümünde kalan sınıfları üzerinde çeşitli olasılık hesabı uygulamaları gerçekleştirilmiştir.

3. BULGULAR

Bu bölümde, bu araştırmanın amacı doğrultusunda, sınırlılıklar bölümünde ifade edilen alanlar içinde ve yöntem bölümünde sunulan matematiksel ve kuramsal alt yapı çerçevesinde gerçekleştirilen olasılık hesaplamaları sunulmuştur.

3.1. Z/n Kalan Sınıflarında Kesişim-Birleşim Olaylarının Olasılığı

Aşağıda sırasıyla seçilen tamsayının Z/n kalan sınıflarının kesişiminde ve birleşiminde bulunma olasılıkları incelenmiştir.

3.1.1.Z/n Kalan Sınıflarında Kesişim Olayının Olasılığı

Z/n örnek uzay olarak alınır. Kalan sınıfları da eş olumlu çıktıları göstersin. Kalan sınıfların her biri bir olaydır ve iki kalan sınıfının kesişim olayının olasılığı, Bağıntı-2'den ötürü sıfırdır. Çünkü, pay kısmında iki kalan sınıfının kesişiminin eleman sayısı yer alacaktır. Herhangi iki kalan sınıf kesin olarak ayrık olduğundan kesişimleri boş küme, dolayısıyla kesişimin eleman sayısı sıfır olur. Sonuç olarak, kesişimin olasılığı 0/n olur ki, n≠ 0 olduğundan olasılık değeri sıfır bulunur.

3.1.2.Z/n Kalan Sınıflarında Birleşim Olayının Olasılığı

Aynı örnek uzayda iki olayın birleşim olayının olasılığı, Bağıntı-3 aracılığıyla hesaplanmaktadır. Z/n kalan sınıflarının kesişim olayının olasılığının sıfır olduğu bulunmuştu. Bu nedenle, ayrık olayların birleşim olasılığı söz konusu olacağından;

Z/n kalan sınıfları içinde herhangi ikisi $\overline{n_1}$ ve$\overline{n_2}$ kalan sınıfları biçiminde gösterilirse bu kalan sınıfların birleşim olaylarının olasılığı;

P($\overline{n_1} \cup \overline{n_2}$) = $p(\overline{n_1})$+ $p(\overline{n_2})$, biçiminde bulunur.

Bununla ilgili, Uygulama-1 bir örnek uygulama olarak sunulmuştur.

Uygulama 1:$Z/5$'te tüm tamsayılar 5 denk sınıfa ayrıldığından seçilen herhangi bir tamsayının 5 ile bölündüğünde söz gelimi iki kalanını verme olasılığı 1/5 olur. Ayrıca, bu beş sınıf ayrık olduğundan bir tamsayının beş ile bölümünden iki farklı kalan elde edilmesi

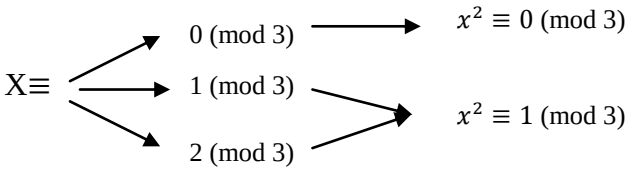
imkânsız olaydır. Bununla birlikte Z/5'te seçilen bir tamsayının 2 veya 3 kalanını vermesi olasılığı;

$P(A \cup B) = P(A) + P(B) - P(A \cap B)$bağıntısında$P(A \cap B) = 0$ olduğu değerlendirilerek;

1/5+1/5=2/5 bulunur.

3.1.3. Modüler Aritmetikte Kare Kalan, Küp Kalan Ve Daha Yüksek Kuvvetlerden Kalanlar İle İlgili Olasılık Hesaplamaları

Bir tamsayının mod 3'te 0, 1 veya 2'ye denktir. Mod 3'te kare kalan sınıfları ise $\{\overline{0}, \overline{1}\}$'dir. Bir başka deyişle, tüm tamsayıların karesi mod 3'te 0 veya 1'e denk olmaktadır. Bunlardan yalnızca 0 kalanını veren tamsayıların (3'ün katı şeklindeki) kareleri mod 3'te tekrar 0 kalanını verir. Mod 3'te 1 veya 2'ye denk olan tamsayıların kareleri mod 3'te 1'e denk olur. Bu durumu ağaç diyagramı ile aşağıdaki biçimde gösterebiliriz.



Kare kalan ve küp kalan ile ilgili Uygulama-2, Uygulama-3, Uygulama-4 ile sunulan bazı olasılık hesaplamaları yapılmıştır.

Uygulama-2: Bir tamsayının mod3'te kare kalanının 1 olma olasılığı kaçtır?

Bu soruya yanıt vermek için 1 kalanının hangi kalan sınıflarından kaynaklandığına bakılarak cevaplanabilir. Bu durumda seçilen bir tamsayının karesinin 1 kalanını bırakması için sayının Z/3'te $\overline{1}$ veya$\overline{2}$ kalan sınıfından gelmesi gerekmektedir. Dolayısıyla bir tamsayının karesinin mod 3'te 1 kalanını vermesi olasılığı 2/3, 0 kalanını verme olasılığı ise 1/3 bulunur.

Olasılıkla ilgili diğer bazı konular (iki olayın kesişimin/birleşiminin olasılığı) kare kalan, küp kalan sınıflarına uygulanabilir.

Not: Örneğin, $Z/7$'de kalan sınıfları göz önüne alınsın.

$Z/7'$de kalan sınıflar $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$'dır.

Dolayısıyla, Mod 7'de X ≡ 0,1,2,3,4,5 ya da 6'dır.

Mod 7'de kare kalanlar ise$0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 2$,$4^2 \equiv 2$, $5^2 \equiv 4$,$6^2 \equiv 1$

Mod 7'de kare kalanların 0, 1, 2 ve 4 ile sınırlı olduğu görülür.

Bir başka deyişle 0 kare kalanı 0'dan,

1 kare kalanı 1 ve 6' dan,

2 kare kalanı 3'ten ve 4'ten

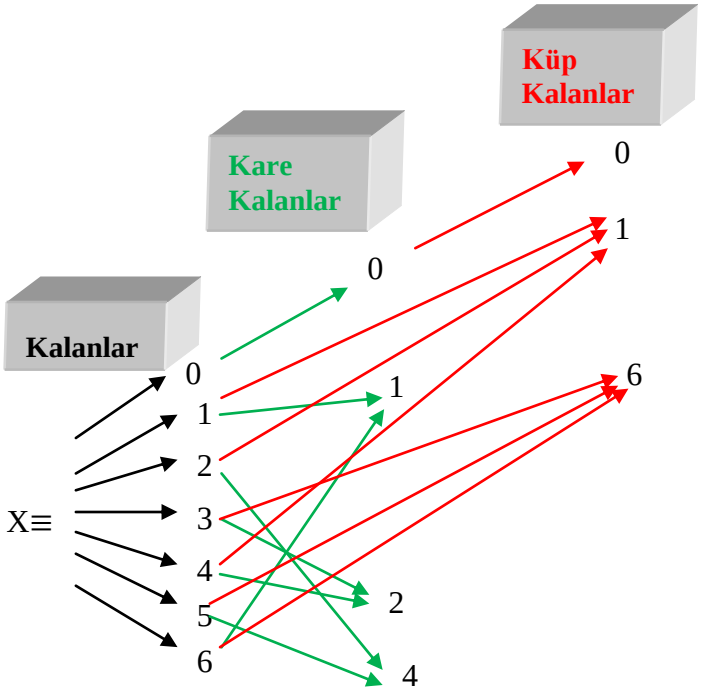
4 kare kalanı ise 2 ve 5'ten kaynaklanmaktadır.

Mod 7'de küp kalanlara göz atarsak;

$0^3 \equiv 0$, $1^3 \equiv 1$, $2^3 \equiv 1$, $3^3 \equiv 6$,$4^3 \equiv 1$, $5^3 \equiv 6$,$6^3 \equiv 6$

Küp kalanların 0,1 ve 6 ile sınırlı olduğunu buluruz.

Mod 7'de kalan, kare kalan ve küp kalanlar için aşağıdaki biçimde bir ağaç diyagramı oluşturulabilir:



Bu kalan grupları ile ilgili şu olasılık uygulamaları gerçekleştirilebilir:

Uygulama-3: Rastgele seçilen herhangi bir tamsayının mod 7'de kare kalanın 2 ve küp kalanının 6 olma olasılığı kaçtır?

Çözüm: Bu problemde kare kalanın ve küp kalanın 6 olmasını sağlayan bir kalan sınıf aranır.

Yukarıdaki diyagram incelendiğinde yalnızca $\overline{3}$ kalan sınıfındaki tamsayıların kare kalanının 2 ve küp kalanının 6 olduğu görülür. Bu nedenle istenen olasılık 1/7'dir.

Uygulama-4: Rastgele seçilen herhangi bir tamsayının mod 7'de kare kalanın 4 veya küp kalanının 1 olması olasılığı kaçtır?

Çözüm: Bu problemde şu olaylar tanımlanabilir.

A={Kare kalanı 4 olan kalan sınıfları}=$\{\overline{2}, \overline{5}\}$

B={Küp kalanı 1 olan tamsayılar}= $\{\overline{1}, \overline{2}, \overline{4}\}$

A∩B={Kare kalanı 4 ve küp kalanı 1 olan tamsayılar}=$\{\overline{2}\}$

Bu durumda $p(A) = 2/7; p(B) = 3/7$ ve $p(A \cap B) = 1/7$'dir.

$p(A \cup B) = p(A) + p(B) - p(A \cap B)$bağıntısı yardımıyla;

İstenen olasılığın cevabı 4/7 bulunur.

3.1.4. Kalan Sınıfları İle Şartlı (Koşullu) Olasılık Uygulaması

Kalan sınıfları ile şartlı olasılığın bir hesaplanışı Uygulama-5'te sunulmuştur.

Uygulama-5: Rastgele seçilen bir tamsayının mod 7'de küp kalanının 6 olduğu bilindiğine göre bu tamsayının kare kalanının 2 olması olasılığı kaçtır?

Çözüm: mod 7'de küp kalanın 6 olması koşulu örnek uzayın bu koşul çerçevesinde küp kalanı 6 olan kalan sınıflarla sınırlar. Bu kalan sınıflar sırasıyla $\{\overline{3}, \overline{5}, \overline{6}\}$'dır. O halde istenen olasılık bu kalan sınıflar üzerinden aranır. Diğer bir deyişle, bu kalan sınıflarından 2 kare kalanı veren sınıflar bulunur. Buna uygun kalan sınıfı $\{\overline{3}\}'$tür. Dolayısıyla;

P(A/B)$=\frac{p(A\cap B)}{p(B)}$ bağıntısı yardımıyla P(A/B) = $\frac{1/7}{3/7}$ = 1/3 bulunur.

3.1.5. Fermat'ın Küçük Teoreminin Kalan Sınıflarında Olasılık Hesabı Bakımından İncelenmesi

Fermat'ın Küçük Teoreminin, kalan sınıflarında olasılık hesabı bakımından nasıl sonuçlar doğuracağı proje kapsamında incelenmiştir. Bu teorem;

p bir asal sayı ve a∈ Z^+ ile p aralarında asal olmak üzere $a^{p-1} \equiv 1\ (modp)$ biçiminde ifade edilmektedir.

Bu teoreme göre, Z/n kalan sınıfında n bir asal sayı olarak alınırsa Z/p asal sınıflarında için aşağıdaki biçimde bazı olasılık incelemeleri yapılabilir.

Z/p'de kalan sınıflar $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{p-1}\}$ olarak gösterilir. Z/p örnek uzay olmak üzere;

Bu kalan sınıflar arasından $\overline{0}$ kalan sınıfı hariç diğer kalan sınıflara ait elemanlar p asal sayısı ile aralarında asaldır. Dolayısıyla, $\overline{0}$ kalan sınıfı hariç diğer kalan sınıflar için Fermat'ın küçük teoremi geçerli olur.

Küçük Fermat teoremi kullanarak Uygulama-6'da sunulmuş olanörnek olasılık uygulaması yapılabilir.

Uygulama-6:$Z/7'dex^6 + y^6 \equiv 1$ olma olasılığı kaçtır?

Çözüm: $Z/7'de$ herhangi bir $\overline{0}$ kalan sınıfı dışındaki sınıflardan alınacak herhangi bir tamsayı için Fermat teoremi uyarınca 6. kuvvetten kalanı 1 olur. $\overline{0}$kalan sınıfından seçilecek bir tamsayının 6. kuvveti ise 0 kalanını verir. Dolayısıyla, 6. kuvvet için 0 veya 1 kalanı dışında bir kalan seçeneği yoktur. Öyleyse;

$Z/7'dex^6 + y^6 \equiv 1$denkliği ile ilgili şu gözlem yapılabilir;

Z/7'de hangi kalan sınıfa ait bir tamsayı alınırsa alınsınbunun 6. Kuvveti Küçük Fermat gereği, 1 veya 0'a denktir. Başka kalan opsiyonu yoktur.

Bu nedenle sorulan denkliğin sağlanması için,

$x^6 \equiv 0 ve y^6 \equiv 1$ (buna A olayı diyelim), veya $x^6 \equiv 1$ ve $y^6 \equiv 0$ (buna B olayı diyelim) olmalıdır.

A olayının olasılığı şu şekilde hesaplanabilir:

$x^6 \equiv 0$olması için $x \equiv 0$ olması gerekir. Bunun olasılığı, Z/7'de 1/7'dir.
$y^6 \equiv 1$olması için Fermat gereği, y tamsayısı Z/7'de yer alan sıfır kalan sınıfı dışındaki sınıflardan birinde bulunmalıdır. Bunun olasılığı ise, 6/7'dir.

Öyleyse; $x^6 \equiv 0$ ve $y^6 \equiv 1$ olma olasılığı çarpma kuralı gereği 1/7.6/7=6/49 olur.

B olayı, A olayı ile simetrik olduğundan B olayının olasılığı da 6/49 olur. Son olarak A veya B olayının olasılığı hesaplanır. Bu olaylar, ayrıktır. Bu nedenle birleşimin olasılığı;

6/49 + 6/49 = 12/49 bulunur.

3.1.6. Euler'in φ fonksiyonunun Kalan Sınıflarında Olasılık Hesabı Bakımından İncelenmesi

Bu çalışma kapsamında bir başka inceleme Euler'in $\boldsymbol{\varphi}$fonksiyonu için yapılmıştır. Bilindiği üzere, $\boldsymbol{\varphi}$fonksiyonu bir doğal sayıyı kendisinden küçük ve kendisiyle aralarında asal olan pozitif tamsayıların sayısıyla eşleştiren fonksiyondur.

$\boldsymbol{\varphi(n)} = \{\boldsymbol{n'den}$ küçü$\boldsymbol{k\ ve\ n\ ile\ aralarında\ asal\ olan\ pozitif\ tamsayıların\ sayısı}\}$

n sayısının asal bölenleri $\alpha_1, \alpha_2, \dots, \alpha_k$ olmak üzere,

$$\boldsymbol{\varphi(n) = n.\left(1-\frac{1}{\alpha_1}\right).\left(1-\frac{1}{\alpha_2}\right)\dots\left(1-\frac{1}{\alpha_k}\right)}$$

a ile n aralarında asal olmak üzere,

$a^{\boldsymbol{\varphi(n)}} \equiv 1\ (mod(n))$bağıntısı bulunmaktadır.

Örneğin, $\boldsymbol{\varphi(100) = 100.\left(1-\frac{1}{2}\right).\left(1-\frac{1}{5}\right) = 40'tır.}$

Bu durumda 100 ile aralarında asal herhangi bir doğal sayının 40. kuvveti 1'dir. Bununla ilgili, Z/100'de Uygulama-7'de sunulan inceleme yapılmıştır.

Uygulama-7: Z/100'de x ile 100 aralarında asal olmak üzere;
$x^{40} + y^{40} \equiv 1\ (mod(100))$ denkliğinin sağlanma olasılığı kaçtır?

Çözüm: $\varphi(100) = 40$ ve x ile 100 aralarında asal olduğu için

$x^{40} \equiv 1\ (mod(100))'$ dür.

Bu verilen denklikte yazılırsa $y^{40} \equiv 0\ (mod(100))$ bulunur.

Buradan $y^{40} = 100.k(k \in Z)$ elde edilir. Bu denklemde k pozitif bir tamsayıdır.y sayısının 2 ve 5 çarpanlarını içermesi gerekli ve yeterlidir.

Z/100'de y'nin kalan sınıf kaynakları 2 ve 5 çarpanlarını içermelidir. Bir başka deyişle 10 ve katları biçiminde kalan sınıfları olmalıdır. Öyleyse bunlar,

$\overline{0}, \overline{10}, \overline{20}, \ldots, \overline{90}$ sınıflarından birinden gelmelidir. Bunun olasılığı $= \frac{10}{100} = \frac{1}{10}$ ′dur.

3.1.7. Modüler Aritmetik Probleminde Olasılık Hesaplanması

Kalan sınıflarının gerçekleşme olasılıklarının incelendiği bu çalışmada son olarak bu tür uygulamaların bir modüler aritmetik probleminde nasıl uygulanabileceği Uygulama-8'de sunulmuştur:

Uygulama-8: İlk seferini Pazartesi günü yapmış olduğu bilinen bir vapur, 3 günde bir sefer yapmaktadır. Rastgele bir günde gelip vapura binen birinin vapura Salı günü binmiş olma olasılığı kaçtır?

Çözüm: Kişinin vapura bindiği gün ile ilgili şu gözlemler yapılabilir:

i) Vapur 3 günde bir sefer yaptığına göre, vapura binilen gün Pazartesiden itibaren 3'ün katı olan bir sayı "3k" olarak gösterilebilecek kadar gün sonrasıdır.
ii) Öte yandan binilen günün Salı olabilmesi için başlangıç günü Pazartesiye göre 7m+1 gün geçmiş olmalıdır.

Gün sayısı A ile gösterilirse;

A = 3k = 7m+1 yazılabilir.

Bu eşitlikte her tarafa 6 eklenirse;

A+6 = 3k+6 = 7m+7 dolayısıyla A+6 hem 3'ün hem de 7'nin katı olur. Öyleyse;

$A + 6 \equiv 0\ (mod(21))$ ise$A \equiv 15\ (mod(21))$ olur.

Sonuç olarak, herhangi bir gün gelerek vapura binen birinin Salı günü binmiş olması geldiği günün başlangıç gününden itibaren 21 modunda 15 kalanı veren kadar gün sonra binmesine bağlıdır. O halde, tüm sayılar Z/21'e göre sınıflanırsa$\overline{15}$ kalan sınıfında bulunan tamsayılar kadar gün sonra vapura binerse Salı günü binmiş olur. Z/21'in 21 kalan sınıfı arasında yalnızca $\overline{15}$ kalan sınıfında istenen durum sağlanacağından olasılığı 1/21 bulunur.

4. TARTIŞMA Ve SONUÇ

Bu çalışmada, "tamsayılar Z/n biçiminde kalan sınıflarına (kalan sınıfları sonsuz elemanlı olacak biçimde) ayrıldığında seçilen her bir tamsayının bu kalan sınıflardan birinde olma olasılığı eşittir" varsayımına dayalı olarak modüler aritmetik kapsamındaki kalan sınıfları, kare kalan-küp kalan, Fermat'ın Küçük Teoremi, Euler'in $\boldsymbol{\varphi}$ fonksiyonu ve modüler aritmetik problemi konularına yönelik bazı olasılık uygulamaları gerçekleştirilmiştir.

Çalışma sonucunda, bu çalışmadaki ilişkilendirme ile sonlu olmayan (Uygulama-8'de görüldüğü gibi sonlu süreye dayalı olmayan) bazı modüler aritmetik problemlerine yönelik olasılık hesaplamaları yapılabildiği anlaşılmıştır. Bu çalışmanın ayrık ve sonsuz elemanlı olan kümelerle ilgili olasılığın kavranması ve geliştirilmesine az da olsa bir katkı sağlaması umulmaktadır.

5. ÖNERİLER

Bu çalışmanın sonuçlarına dayalı olarak şu öneriler ileri sürülmüştür;

- Sonsuz elemanlı ayrık kümeleri ile modüler aritmetikteki kalan sınıfları arasında fonksiyonlar kurularak çeşitli olasılık incelemeleri yapılabilir.
- Bu çalışmada temele alınan aksiyom üzerinden veya yeni aksiyomlar geliştirerek ilişkilendirmenin boyutları genişletilebilir.

- Bu çalışma ile kurulan ilişkinin hangi günlük hayat problemlerine uygulanabileceği ile ilgili gözlemler, daha detaylı problem üretimleri ve çözümleri içeren çalışmalar yapılabilir.
- Olasılığın modüler aritmetik ile ilişkisini her iki alanın kavramlarını daha da çeşitlendirerek ilişkilendiren detaylı çalışmalar yapılabilir.
- Matematikte çeşitli alanları ilişkilendiren projeler hazırlanarak günlük hayat problemleri yeni bakış açıları ile incelenebilir, bu durum ortaöğretim öğrencilerinin ilişkili düşünme becerilerinin gelişimine katkı sağlanabilir.

Kaynakça

URL-1:http://www.webmastersitesi.com/bilmediklerimiz/248895-matematikte-olasiligin-tarihi-nedir.htm (erişim tarihi: 16/10/2016).

URL-2:http://www.ebilge.com/6703/Moduler_aritmetik_nasil_ortaya_cikmistir.html(erişim tarihi: 17/10/2016).

URL-3:http://kisi.deu.edu.tr/kemal.sehirli/BOLUM_1.pdf (erişim tarihi: 16/10/2016).