BATI ANADOLU
EĞİTİM BİLİMLERİ DERGİSİ
http://web.deu.edu.tr/baed
Dokuz Eylül Üniversitesi Eğitim Bilimleri Enstitüsü

ISSN 1308 – 8963

Cilt: 01, Sayı: 03, 2011, 19-43

ŞİFRELEME ETKİNLİKLERİYLE FAKTÖRİYEL VE PERMÜTASYON KONUSUNUN ÖĞRETİMİ

TEACHING FACTORIAL AND PERMUTATION TOPICS THROUGH CODING ACTIVITIES

[a]Ahmet Ş. ÖZDEMİR [b]Fatma ERDOĞAN

[a]Doç.Dr., Marmara Üniversitesi Atatürk Eğitim Fakültesi Matematik Eğitim A.B.Dalı,

e- mail:ahmet.ozdemir@marmara.edu.tr

[b]Öğretmen, Fatma Süslügil İlköğretim Okulu, e-mail: fatmaerdogan83@gmail.com

Özet

Öğrencilerin yaşanılan hızlı bilgi dönüşümüne yabancı kalmalarını önlemek amacıyla, ilköğretim seviyesinden itibaren şifreleme yöntemlerine öğretim etkinliklerinde yer verilmesi önemlidir. Bu araştırmada, ilköğretim yedinci sınıf faktöriyel ve permütasyon konusunun öğretiminde kullanılabilecek şifreleme etkinlikleri tasarlamak ve etkinliklerin kullanıldığı sınıf içi atmosferini gözlemleyerek gelişen eğitimsel olayların incelenmesi amaçlanmıştır. Verilerinin toplanması, çözümlenmesi ve yorumlanmasında nitel araştırma yöntemi benimsenmiştir. Araştırmada gözlemle veri toplama tekniklerinden video kaydı ve yazılı kaynaklardan yararlanılmıştır. Araştırma, 2008-2009 öğretim yılı güz döneminde, İstanbul ili Zeytinburnu ilçesindeki bir ilköğretim okulunda okuyan 10 yedinci sınıf öğrencisi ile gerçekleştirilmiştir. Araştırma sonucunda, öğrencilerin şifreleme ile tanıştığı, şifrelemelerde kullanılacak matematiksel kavramların ve işlem becerilerinin kazanıldığı belirlenmiştir. Şifreleme ve deşifre etkinlikleri aracılığıyla, öğrencilerin faktöriyel ve permütasyon kavramlarını öğrenip, uygulamalar yaptıkları saptanmıştır.

Anahtar kelimeler: Matematik Öğretimi, Şifreleme, Faktöriyel, Permütasyon

Abstract

Coding techniques in teaching activities is important starting from primary school level to prevent students from staying behind the quick transformation of information. The aim of this study is to design coding activities which can be used in Elementary School seventh grade factorial and permutation teaching, and to examine educational activities by observing classroom atmosphere that these activities are used. Qualitative research method was adapted to gather, analyze and interpret data. In the

research, video recording and written documents were utilized as observational data gathering techniques. The implementation of the research was performed in the 2008-2009 education year fall semester, with 10 seventh grade students at a elementary school in Zeytinburnu district of İstanbul. At the end of the research, it was found that the students have been familiar with coding, and they have gained the ability of using mathematical concepts and operation skills to be used in coding. It was detected that the students have been learned factorial and permutation concepts and performed practices by the help of coding and decoding activities.

Key words: Mathematics Education, Coding, Factorial, Permütation

GİRİŞ

Her alanda olduğu gibi eğitim alanında ve toplum yaşamında matematiğin yeri ve önemi giderek artmaktadır. Matematiğin artan önemine karşın, ülkemizde öğrencilerin matematik dersindeki başarıları genelde düşüktür ve bu ders pek çok öğrenci için sevimsiz, zor, soyut ve sıkıcıdır (Arslan, 1994).

Ülkemizde ilköğretimin, biri öğrencilere hayat için gerekli olan temel becerilerin kazandırılması; diğeri, ortaöğretime öğrenci hazırlaması olmak üzere iki temel görevi vardır (Baykul, 2005). Bu amaçların gerçekleşmesi için etkili akıl yürütme, eleştirel düşünme ve problem çözme gibi önemli zihinsel süreçlerin öne çıkarılması gerekmektedir. Bu noktada, matematik öğretiminin önemi ortaya çıkmaktadır (Baykul, 2005). Eğitimde eleştirel düşünmenin uygulama alanları olarak Brown (1997) eleştirel düşünmenin farklı alanlara uygulanmasının, ders planlarının hazırlanması ve öğrenme etkinliklerinin düzenlenmesi ile olabileceğini belirtmektedir. Öğrencilere, konuları anlamlı öğrenmelerini sağlayacak şekilde öğrenme ortamları hazırlanmadıkça onların düşünme yeteneklerinin gelişmesinin beklenemeyeceğini, ancak gerçek yaşam durumlarının kullanılması halinde aktif katılımın sağlanacağını belirtir (Demirel, 2004).

Matematiksel bilgiler birbiriyle ilişkili olduğundan dolayı tam anlaşılmayan bir konu diğer konuların öğreniminde güçlükler doğuracaktır (Altun, 2004). Boyacıoğlu, Erduran ve Alkan (1996)'ın yaptığı araştırmaya göre, matematik konuları içerisinde "Permütasyon ve Olasılık" konusu hem öğretmenler hem de öğrenciler açısından en problemli konuların başında gelmektedir. Bu araştırmanın sonuçlarına göre, öğrencilerin %91'i anlamakta zorluk çektikleri konular sıralamasında, öğretmenlerin de %84'ü işlenmesi en zor konular içinde ilk sıraya yerleştirmişlerdir.

Permütasyon ve faktöriyel konuları olasılık gibi diğer konulara da temel teşkil etmektedir. Konunun öğretimindeki güçlükleri giderme amacıyla öğrencilerin derse aktif katılımını sağlayan farklı öğretim yöntem ve teknikleriyle öğretim ortamları düzenlenmiş ve öğrenci

başarısında olumlu yönde değişim olduğu belirlenmiştir (Bulut, 1994; Çubuk, 2004; Ekinözü, 2003; Ercan, 2008; Öztürk, 2005; Şengül ve Ekinözü, 2006, 2007; Yazıcı, 2002). Yazıcı (2002)'nın çalışmasında, permütasyon ve olasılık konusu buluş yöntemine uygun çalışma yapraklarıyla öğretilmiştir. Araştırmanın bulguları, buluş yoluyla öğretimin permütasyon ve olasılık konusundaki başarıyı olumlu yönde etkilediğini, öğrencilerin motivasyonunu artırarak derse aktif katılımlarını sağladığını göstermiştir. Şengül ve Ekinözü (2006, 2007) araştırmalarında, permütasyon ve olasılık konusunun öğretiminde canlandırma yönteminin kullanılmasının öğrenci başarısına, hatırlama düzeyine ve matematik tutumlarına etkilerini incelemişlerdir. Deney ve kontrol grupları arasında, öğrenci başarıları yönünden anlamlı bir farklılık bulanamamasına rağmen canlandırma yönteminin öğrencilerin hatırlama düzeyleri üzerinde etkili olduğu görülmüştür. Ayrıca, öğrencilerin matematik dersine yönelik tutumlarında olumlu değişmeler sağlanmıştır.

Şifreleme

Gelişen bilgi ve teknolojinin sonucu olarak, ülkeler arasında güvenli bir hayatın sağlanması açısından rekabet artmış; bilgi aktarımının gizlilik ve güvenliği önem kazanmıştır. Bu durum, bilgi iletişiminde gizliliğin sağlanmasını amaçlayan şifre biliminin (Kriptoloji) hızla gelişerek yaygınlaşmasına neden olmaktadır. Şifre bilimi, kriptoloji ve kripto analiz olarak iki ana bölüme ayrılır. Gerçek metnin şifreli metne dönüştürülmesi için yapılan işlemler, oluşturulan sistemler, fonksiyonlar ve algoritmalar ile yani şifreleme ile ilgilenen çalışma alanına kriptografi adı verilir. Kripto analiz ise şifreli mesajları okumaya çalışmaktır (Jacobsen, 1995).

Bilgi güvenliği için geliştirilen sistemler içerisinde şifreleme ve şifreleme algoritmaları önemli bir işleve sahiptir. Ticari ilişkilerde, devlet işlerinde, askeri işlerde ve personel ilişkilerinde güvenli bilgi akışının sağlanması için şifreleme önemlidir. Günlük yaşamın temel gereksinimleri olan güvenlik ve gizliliğin sağlanmasında vazgeçilmez bir unsur olan şifreleme ve şifreleme algoritmalarının, matematiksel bir temeli vardır. Şifreleme algoritmalarının matematiksel modellemelerinde bir çok matematik kavram ve konusundan yararlanılır. Modüler aritmetik, asal sayılar, fonksiyonlar, obeb örnek olarak gösterilebilir.

Şifrelemenin tarihi yüzlerce yıl öncesine dayanmaktadır. Eski Roma İmparatoru Julius Caesar, Sezar (Caesar) şifreleme olarak bilinen en eski ve simetrik anahtar şifrelemenin klasik bir örneği olan basit bir yerine koyma şifrelemesini kullanmıştır (Stallings, 1998). Bu yöntemde alfabedeki her bir harf 3 sonraki harf ile şifrelenir. Türkçe için anahtar, Tablo 1'de gösterildiği gibi 3 harfin ötelenmesiyle oluşturulmuştur. Şifreleme ve şifre çözme işlemleri yapılırken açık metin ile birlikte bir de anahtar kullanılmaktadır. Bir metni şifrelerken kullanılan değiştirme veya dönüştürme metodu anahtardır ve açık metin bu anahtardan yararlanılarak şifrelenmektedir.

Tablo 1. Sezar (Caesar) şifrelemesi

Düz	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
Anahtar	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C

Anahtarın alfabenin k harf ötelenmesiyle elde edildiği varsayılırsa, 29 harften oluşan Türk Alfabesi için anahtar, yani k, 1'den 29'a kadar değer alabilir. Olası bütün anahtarlar denenerek, en fazla 29 denemede şifreli metin kolaylıkla çözülebilir. Dolayısıyla, yerine koyma şifrelemesinin 29 olası anahtar ile güvenli olmaktan uzak olduğu söylenebilir. Yerine koymalı şifrelemede anahtar oluşturulurken alfabedeki her bir harf rast" 1gele bir başka harf ile değiştirilirse anahtar uzayı arttırabilir. Çizelge 1'deki anahtar satırı, alfabedeki 29 harfin herhangi bir permütasyonu olarak değiştirildiğinde anahtar uzayı büyüklüğü 29! olacaktır. Bu durumda olası her anahtarı deneyerek çözüme ulaşma imkansız görünmektedir (Karaahmetoğlu, 2010).

Matematik ile günlük yaşam arasındaki bağlantının kurulması ve öğrencilerin gelecek yaşantıları için temel oluşturulması matematik öğretiminin hedeflerindendir. Bu hedefe ulaşmak için, yurtdışında yapılan birçok çalışmada şifrelemeye matematik öğretimi içerisinde etkinlikler olarak verilmiştir (Bachman, Ezra ve Norton, 2010; Chua, 2006, 2008; Evered ve Gningue, 2001; Hall, 2003; Hamilton ve Yankosky, 2004; www.purdue.edu/discoverpark/gk12/downloads/Cryptography.pdf.; Myerscough ve diğerleri, 1996; Kaur, 2008).

Myerscough ve diğerleri (1996) fonksiyonlar, modüler aritmetik, eşitlik çözümleri, problem çözme stratejilerini geliştirmek gibi birçok konunun öğretiminde kullanılabilecek şifreleme aktiviteleri tasarlamışlardır. Evered ve Gningue (2001) çalışmalarında, öğrencileri temel şifreleme ve deşifre etme teknikleriyle tanıştırmışlardır. İlköğretim seviyesinde gerçekleştirilen çalışma sonucunda, şifreleme ve deşifre etkinlikleri sürecinde öğrencilerin derse ilgilerinin arttığı gözlemlenmiştir.

Chua (2006), Sezar şifreleme tekniklerini kullanarak matris öğretiminde kullanılabilecek bir etkinlik tasarlamıştır. Bu etkinliklerin uygulanması sonucunda, öğrencilerin şifreleme ve deşifre yapabildikleri belirlenmiştir. Ayrıca, bu etkinlikleri kullanan öğretmenlerin kavram öğretme sürecini daha kolay ve verimli gerçekleştirmeleri beklenmektedir. Benzer şekilde, Chua (2008) şifrelemeyi temel alan, fonksiyonların pratik uygulamaları ve ters fonksiyonları içeren öğretim etkinlikleri tasarlamıştır.

Ancak, ülkemizde şifreleme üzerine yapılan çalışmalar incelendiğinde şifreleme ve matematik algoritmaları, analizleri ve şifreleme tasarıları üzerine yoğunlaşıldığı (Başar, 2004; Buluş, 2006; Çalışkan, 2004; Karaahmetoğlu, 2010; Tuncal, 2008) görülmektedir. Matematik öğretiminde şifrelemenin kullanılmasıyla ilgili çalışmalar ise sınırlı sayıdadır (Güler, 2007; Özdemir ve Güler, 2008; Saygı ve Umay, 2010). Güler'in (2007) şifreleme etkinliklerini kullanarak modüler aritmetik konusunun öğretimini gerçekleştirdiği görülmüştür. Bu araştırmanın bulguları, modüler aritmetik konusunun öğretiminde şifreleme aktiviteleri kullanılmasının matematik başarısını olumlu yönde etkilediğini göstermektedir. Saygı ve Umay (2010) "Kriptoloji Yardımıyla Fonksiyon Kavramının Oluşturulması" adlı çalışmayı gerçekleştirmişlerdir. Bu çalışmalarında, şifrelemeden yararlanarak fonksiyon ve ters fonksiyon konularının öğretilmesinde kullanılabilecek etkinlikler tasarlamışlardır. Çalışmalarında, şifrelemenin öğrencilere fonksiyon kavramının kazandırılmasında öğretici olduğu kadar eğlenceli de bir yol olabileceği ifade edilmiştir. İlköğretim seviyesinden başlanarak şifreleme etkinliklerinin kullanıldığı çalışmaların yapılması önem kazanmaktadır.

Araştırmanın önemi ve amacı

Özellikle 2003'lerden sonra yoğunluk kazanan ilköğretim programlarını yenileme çalışmaları sonucu 2005–2006 eğitim öğretim yılından itibaren ilköğretim 1–5. sınıflar düzeyinde bütün okullarda; 6–8. sınıflarında ise 2006–2007 öğretim yılından itibaren 6. sınıflardan başlanarak kademeli şekilde uygulanmaya başlanmıştır. Yeni ilköğretim programlarının uygulanmasıyla birlikte katı davranışçı öğrenme anlayışından, yapılandırmacı bir yaklaşıma geçilmiştir (MEB, 2005).

Yapılandırmacı yaklaşım kapsamında, öğrenenler yeni bilgi ile eski bilgi arasında bağlantılar kurarlar. Öğrenciler yeni bilgileri karşılaştırır, sorgular, inceler ve kabul ederler (Cooperstein ve Kocevar-Weidinger, 2004). Matematik konularının diğer derslere göre daha güçlü bir sıralı yapıya sahip olduğu (Altun, 2004) düşünüldüğünde birbiriyle önşartlılık ilişkisi içinde olan konuların öğrenilmesi önemlidir.

Ülkemizde faktöriyel ve permütasyonun öğretimiyle ilgili yapılan araştırma sonuçlarına göre, faktöriyel ve permütayon konusunun gerçek hayatta ve çeşitli bilim dallarında önemli bir yere sahip olmasına karşın konunun öğretiminde güçlüklerle karşılaşıldığı belirlenmiştir (Bulut, 1994; Çubuk, 2004; Ekinözü, 2003; Öztürk, 2005; Şengül ve Ekinözü, 2006, 2007; Yazıcı, 2002). Konunun öğretiminde farklı öğretim etkinliklerinin kullanılması gerekliliği ortaya çıkmıştır.

Matematik yaparken akıl yürütme becerilerinin geliştirilmesi için ortamlar hazırlanmalıdır (MEB, 2007). İlköğretimde matematik öğretiminin gözlem, yaşantı ve sezgiye dayalı olması gerektiği düşünüldüğünde görsel ve somut araç-gereçleri içeren, öğrencileri düşünmeye, mantıksal çıkarım yapamaya sevk eden etkinliklere yer verilmesi önemlidir. Matematiksel

temelleri olan şifreleme yöntemleri, akıl yürütme becerilerinin kullanımını da gerektirmektedir.

Şifreleme, matematiğin günlük hayatta kullanımını ve teknoloji bağlantısını da vurgular. Bu öneminden dolayı yurtdışı birçok çalışmada matematik öğretiminde şifrelemeye yer verilmiştir. Bu çalışmalarda, ilkokuldan üniversiteye kadar çeşitli öğretim basamaklarında şifreleme yardımıyla matematiksel kavramların derinlemesine öğretimi gerçekleştirilmiştir. Ayrıca, öğrencilerin matematik dersine olan ilgilerinde artma gözlenmiş ve tutumlarında olumlu yönde gelişmeler belirlenmiştir (Bachman, Ezra ve Norton, 2010; Chua, 2006, 2008; Evered ve Gninque, 2001; Hall, 2003; Hamilton ve Yankosky, 2004; Kaur, 2008; McCartney, 2000; Myerscough ve diğerleri, 1996). Ülkemizde ilköğretim seviyesinde şifrelemenin matematik öğretiminde kullanıldığı çalışmaların sınırlı olduğu dikkat çekmektedir (Güler, 2007; Özdemir ve Güler, 2008; Saygı ve Umay, 2010).

Öğrencilerin yaşanılan hızlı bilgi dönüşümüne yabancı kalmalarını önlemek amacıyla, ilköğretim seviyesinden itibaren şifreleme yöntemlerine öğretim etkinliklerinde yer verilmesi önemlidir. Öğrencilerin hem şifreleme kavramı hem de yerine koyma şifrelemesiyle tanışmalarını sağlayan; şifreleme etkinlikleri aracılığıyla faktöriyel ve permütasyon konusunun öğretimini gerçekleştiren bir çalışma yapılmıştır. Teoriden ziyade öğretmenlerin gerçek sınıf ortamlarında uygulayabilecekleri, öğrencilerin derse aktif katılımlarını sağlayacak, sorgulayıcı ve yaratıcı şifreleme etkinlikleri tasarlanmıştır. Bu yönüyle bu araştırmanın alan yazındaki önemli bir açığı kapatacağı düşünülmektedir.

Bu araştırmada, ilköğretim yedinci sınıf faktöriyel ve permütasyon konusunun öğretiminde kullanılabilecek şifreleme etkinlikleri tasarlamak ve etkinliklerin kullanıldığı sınıf içi atmosferini gözlemleyerek gelişen eğitimsel olayların incelenmesi amaçlanmıştır.

YÖNTEM

Araştırmanın deseni

Bu araştırmanın verilerinin toplanması, çözümlenmesi ve yorumlanmasında nitel araştırma yöntemi benimsenmiştir. Bu araştırmada nitel araştırma tekniklerinden olan durum çalışmasıdır. Durum, bir program, bir olay, bir aktivite veya zaman ve yerle sınırlı bir grup birey olabilmektedir (McMillan ve Schumacher, 2001). Araştırmada gözlemle veri toplama tekniklerinden video kaydı ile yazılı kaynaklardan yararlanılmıştır. Veri toplama araçları ve toplanan verilerin analiz ve yorumlanmasında benimsenen sürekli karşılaştırma yöntemi kullanılmıştır.

Çalışma grubu

Yukarıda bahsedilen temel amaç çerçevesinde araştırma, 2008-2009 öğretim yılı güz döneminde, İstanbul ili Zeytinburnu ilçesinde Fatma Süslügil İlköğretim Okulu'nda okuyan 10 yedinci sınıf öğrencisi ile gerçekleştirilmiştir. Okuldaki yedinci sınıf şubelerine dersi olan öğretmenlerle görüşülmüştür. Öğrenci kişisel dosyaları incelenerek ailelerin sosyo-ekonomik bakımından orta seviye aile grubuna girdikleri tespit edilmiştir. Beş yedinci sınıf şubesinden bir sınıf rastlantısal olarak seçilmiştir. Çalışmaya katılacak öğrencilerin seçiminde amaçlı örnekleme yöntemlerinden birisi olan maksimum çeşitlilik örneklemesi kullanılmıştır (Yıldırım ve Şimşek, 2005). Bu örneklemedeki amaç, göreli olarak küçük bir örneklem oluşturmak ve bu örneklemde çalışılan probleme taraf olabilecek bireylerin çeşitliliğini maksimum derecede yansıtmaktır (Yıldırım ve Şimşek, 2005). Öğrencilere daha önce öğrendikleri bilgileri sorgulayan bir başarı testi yapılmıştır. Öğrenciler başarı testi puanlarına göre büyükten küçüğe doğru sıralanmıştır. Maksimum çeşitliliğin sağlanması için başarı yönünden yüksek, orta ve düşük öğrenciler seçilerek heterojen ikili gruplar oluşturulmuştur. Gruplar oluşturulurken cinsiyet bakımından da heterojen olmasına dikkat edilmiştir.

Veri toplama araçları

Araştırmada gözlemle veri toplama tekniklerinden video kaydı ve yazılı kaynaklardan yararlanılmıştır. Şifreleme etkinlikleriyle faktöriyel ve permütasyon konusunu öğretme sürecini incelemek amacıyla video kayıtları tutulmuştur. Araştırma sürecinde öğrenci etkinliklerinden oluşan yazılı dokümanlar çalışma sonunda öğrencilerden alınmıştır. Bu yazılı dokümanlar ders işleme süreci ve öğrencilerin düşünceleri hakkında genel bir fikir vermeleri amacıyla kullanılmıştır.

Yazılı dokümanları oluşturma sürecinde öncelikle literatür taraması yoluyla şifreleme, yerine koyma şifrelemesi, etkinlik temelli öğretim, faktöriyel ve permütasyon konusunun öğretimi amacıyla gerçekleştirilmiş olan araştırmalar incelenmiştir (Chua, 2006; Ekinözü, 2003; Evered ve Gningue, 2001; Hall, 2003; Jacobsen, 1995; Öztürk, 2005; www.cimpt.plymouth.ac.uk/resources/codes/codes_u1_1p.pdf.).

Yurtdışında yapılan çalışmalar, araştırmacılar ve Marmara Üniversitesi'nde görev yapan yabancı dil alanında uzman bir öğretim üyesi tarafından bağımsız olarak Türkçe'ye çevrilmiştir. Çeviriler iki araştırmacı ve yabancı dil alanında uzman öğretim üyesiyle birlikte incelenerek gerekli düzeltmeler yapılmıştır.

Yapılan çeviriler ve yurtiçi kaynaklara (Başar, 2004; Buluş, 2006; Çalışkan, 2004; MEB, 2007; Öztürk, 2005; Şengül ve Ekinözü, 2006) dayanılarak araştırmacılar ve Marmara Üniveristesi'nde görevli matematik öğretimi alanında uzman iki öğretim üyesi tarafından şifreleme ve yerine koyma şifrelemesiyle ilgili kazanımlar belirlenmiştir.

Kazanımlar belirlendikten sonra, araştırmacılar tarafından kazanımlara uygun etkinlikler geliştirilmiştir. Etkinliklerin belirlenen kazanımlara ve yedinci sınıf seviyesine uygunluğunu belirlemek amacıyla Marmara Üniveristesi'nde görevli matematik eğitimi alanında uzman bir öğretim üyesi ve ilköğretim okullarında görev yapan üç matematik öğretmeninin görüşlerine başvurulmuştur. Uzmanların görüşlerini almadan önce şifreleme ve yerine koyma şifrelemesiyle ilgili bilgi verilmiştir. Çalışma grubu dışında farklı bir sınıftan rastlantısal olarak seçilen 12 öğrenciyle pilot çalışma yapılmıştır. Bu çalışmanın sonucunda öğrencilerin yaşadıkları zorluklar belirlenmiş ve bunların giderilmesine çalışılmıştır. Öğretmenler, uzmanın görüşleri ve pilot çalışma doğrultusunda yapılan düzeltme işlemlerinden sonra etkinliklere son hali verilmiştir.

Etkinlikler 3 başlıkta toplanmıştır. Etkinliklerde kullanılmak üzere şifreli harf çizelgeleri, Vigenere karesi, frekans çizelgeleri gibi materyallerden oluşan çalışma kağıtları araştırmacılar tarafından hazırlanmış ve uygulama sürecinde öğrencilere dağıtılmıştır. Vigenere karesi tüm harf ötelemelerinin yer aldığı bir çizelgedir (Singh, 1999). Çalışma kağıtlarından alıntılar bulgular bölümünde açıklanarak verilmektedir.

Ayrıca, öğretmenin ders işleme sürecinde gerçekleştirdiği etkinliklerin incelenmesi amacıyla gözlem formu kullanılmıştır. Ders gözlem formu ilköğretim matematik dersi öğretim programından yararlanılarak hazırlanmıştır.

Nitel araştırmada, geçerliğin ve güvenirliğin sağlanmasında kullanılan önemli stratejilerden biri "çeşitleme"dir (Yıldırım ve Şimşek, 2005). Nitel araştırmada gözlem ve görüşmenin olanaklı olmadığı durumlarda veya araştırmanın geçerliğini artırmak amacıyla, görüşme ve gözlem yöntemlerinin yanı sıra, çalışılan araştırma problemleriyle ilişkili yazılı ve görsel materyal ve malzemeler de araştırmaya dâhil edilebilir. Bu demektir ki, doküman incelemesi veya analizi tek başına bir araştırma yöntemi olduğu gibi, diğer nitel yöntemlerin kullanıldığı durumlarda ek bilgi kaynağı olarak da işe yarayabilir (Yıldırım ve Şimşek, 2005). Araştırmada geçerlik ve güvenirlik için öncelikle verileri toplarken veri çeşitlemesi stratejisi kullanılmıştır. Birden fazla veri toplama yöntemi kullanılmış ve toplanan veriler birbirini destekleyici ve teyit edici biçimde sunulmaya çalışılmıştır.

Nitel araştırmada gerek dış gerekse iç güvenirlik kapsamında alınması gereken önlemler vardır. Bu önlemler araştırmacının, kullandığı stratejileri daha belirgin hale getirmesi ve bu şekilde diğer araştırmacıların bu stratejileri benzer biçimde kullanabilmesine olanak sağlamasına ilişkindir (Yıldırım ve Şimşek, 2005). Bu çalışmada, araştırmacılar takip edilen süreçleri açık bir biçimde tanımlamış ve ilgili dokümanlarla desteklemiş, araştırmayı belirli bir sistem içinde aşama aşama geliştirmiş ve bunları sunmuş, veri analizinde kullanılan

kavramsal çerçeveyle ilgili ayrıntılı açıklamalarda bulunmuş, araştırmaya ilişkin gerektiğinde başka araştırmacıların da kullanabileceği bir veri tabanı oluşturmaya çalışmıştır.

Veri toplama süreci

Etkinliklerin uygulanması 6 ders saati sürmüştür. Etkinliklerle ilgili her öğrenciye ayrı çalışma kağıdı verilmiştir. Böylece, her öğrenciye kendi hızına uygun çalışma imkanı sağlanmaya çalışılmıştır. Ancak, bazı etkinlikler düzenlenirken öğrenciler arasındaki etkileşime önem verilerek, öğrencilerin ikişer kişilik gruplar halinde çalışmaları sağlanmıştır. Böylece, işbirliğine dayalı öğrenme kullanılmıştır. Öğrencilerin aktif katılımlarının sağlanması için her öğrenci tartışmalara katılma yönünde cesaretlendirilmiş, yorumlar doğru veya yanlış şeklinde öğretmen tarafından değerlendirilmemiş, ortak kararlara varılmıştır. Uygulama esnasında öğrencilerden sahip oldukları tüm bilgilerden faydalanarak etkinliklerde yer alan sorulara yönelik cevaplarını çalışma kağıtlarına ayrıntılı olarak açıklamaları istenmiştir. Çalışma kağıdı sonuna "Bu çalışma hakkındaki düşüncelerim" bölümü eklenerek, bu kısma öğrencilerden çalışma sonunda şifreleme, faktöriyel ve permütasyon etkinlikleriyle ilgili görüşlerini yazmaları istenmiştir. Etkinliklerin uygulanması süreci video kaydına alınmıştır.

Araştırmada uygulanan etkinliklere yönelik kazanımlar ve açıklamalar aşağıda ayrıntılı olarak verilmiştir.

Birinci etkinlik: Şifrelemeyle tanışalım

Kazanımlar

- Şifreleme kavramını açıklar.
- Şifrelemenin önemini ve günlük hayatta kullanımını belirler.
- Sezar(Caeser) şifrelemesiyle şifreleme ve deşifre yapar.

Uygulama

- Şifreleme kavramının ortaya çıkışı, önemi ve günlük hayatta kullanımı tartışılır.
- Sezar şifrelemesi anlatılır.
- Türk Alfabesi Sezar şifrelemesine göre düzenlenir.
- Metinler Sezar şifrelemesi kullanılarak şifrelenir ve deşifre edilir.

İkinci etkinlik: Şifreleme ve deşifre yapalım

Kazanımlar

- Yerine koyma şifrelemesini açıklar.
- Farklı anahtarlarda şifreleme ve deşifre yapar.
- Deşifre stratejilerini tartışır.

Uygulama

- Harflerin kaç farklı miktarda ötelenebileceği tartışılır.
- Harflerin farklı miktarlarda ötelendiği yerine koyma şifrelemesi anlatılır.
- Farklı anahtarlar kullanılarak metinler şifrelenir ve şifreli metinler deşifre edilir.
- Deşifre etmedeki güçlükler ve daha kolay deşifre etme yolları tartışılır.

- Tüm ötelemeler kullanılarak oluşturulan Vigenere Karesi deşifre etmek için kullanılır.
- Vigenere Karesinin avantajları ve dezavantajları tartışılır.
- Şifreli metinleri deşifre ederken sesli harflerin sessiz harflerle olan ilişkilerinden nasıl faydalanılabileceği üzerine fikir yürütülür.
- Öğretmen tarafından "Türkçe metinlerde harf frekansı" ödevi verilir. Bu ödevde, Türkçe bir metinde en sık kullanılan harflerin sıralandığı bir alfabe oluşturulması istenir.

Üçüncü etkinlik: Şifreleme kullanarak faktöriyel ve permütasyon öğrenelim

Kazanımlar

- Doğal sayıların faktöriyellerini bulur.
- Permütasyon kavramını açıklar ve hesaplar (MEB, 2007).

Uygulama

- İkinci etkinliğin devamı olarak, harflerin kullanılma frekanslarına göre Türkçe alfabe düzenlenir ve deşifre amacıyla bu alfabe kullanılır.
- Öğrenciler tarafından, kare, daire ve üçgensel bölge şeklindeki 3 harften oluşan Martin alfabesindeki her bir harfin rasgele bir başka harf ile değiştirilmesiyle kaç farklı anahtar oluşturulabileceği tartışılır.
- Öğrencilerden 4 ve 5 harfli alfabeler ve yukarıda açıklandığı şekilde anahtar oluşturmaları istenir.
- 29 harften Türk alfabesindeki her bir harfin rasgele bir başka harf ile değiştirilmesiyle oluşturulabilecek anahtar sayısı tartışılır ve ortaya çıkabilecek sonuçlar tahtaya yazılır.
- n tane harften oluşan bir alfabe için bu şekilde kaç farklı anahtar oluşturulabileceği tartışılır.
- Bulunan cevapların matematiksel olarak daha kolay nasıl gösterilebileceği tartışılır.
- Faktöriyel kavramına sınıfla birlikte ulaşılır ve faktöriyel sembolü açıklanır. Farklı doğal sayıların faktöriyellerini bulma uygulamaları yapılır.
- Belirli sayıda elemanın her farklı sıralanışına bu elemanların bir permütasyonu denildiği vurgulanır.

Etkinliklerin uygulanması ve etkinlikle ilgili ders gözlem formunun tutulması araştırmacılar tarafından gerçekleştirilmiştir. Video çekimleri ise sınıfa bir kameranın sabit yerleştirilmesiyle gerçekleştirilmiştir.

Verilerinin analizi ve kullanılan istatistiksel teknikler

Uygulama sonrasında öncelikle tüm veriler bir araya getirilmiştir. Ders etkinliklerinin yer aldığı video kaydı çözümlemesi sürecinde, görüntüler ve konuşmalar yazılı doküman haline getirilmiştir. Bundan sonraki aşamada, yazılı dokümanı kontrol etmek amacıyla görüntüler her iki araştırmacı ve Marmara Üniversitesi'nde görev yapan matematik öğretimi alanında uzman bir öğretim üyesi tarafından tekrar izlenmiştir. Görüntüler ve yazılı doküman karşılaştırılmış, gerekli düzeltmeler yapılmıştır. Etkinlikler öncesinde, sürecinde ve sonrasında

gerçekleşen olaylar hakkında analizlerde bulunulmuştur. Video kayıtlarından elde edilen veriler, yazılı dokümanlar ve ders gözlem formundan elde edilen verilerle düzenlenerek analiz edilmiştir.

Öğrencilerin, faktöriyel ve permütasyon konusunun şifreleme etkinlikleriyle öğretimi sürecinde yapmış oldukları etkinliklerden oluşan çalışma kağıtları yazılı doküman olarak toplanan veri kaynaklarıdır. Çalışma kağıtlarında yer alan şifreleme, faktöriyel ve permütasyon etkinlikleri ve değerlendirme sorularına verilen cevaplara odaklanılarak öğrencilerin nasıl akıl yürüttükleri üzerine düşünülmüş ve daha sonra çalışma kağıdında yer alan ifadeler analiz edilmiştir. Alınan yazılı dokümanlar ihtiyaç duyulan durumlarda aynen alıntı yapılarak ya da yazılı dokümana atıfta bulunarak analizi ve yorumları yapılmıştır.

Verilerin analizi ve yorumlanmasında araştırılan konuyu açıklayıcı, verilerin yüksek bir seviyede yorumlanmasını sağlayan "Sürekli Karşılaştırma Yöntem"i benimsenmiştir. Sürekli karşılaştırmalı veri analiz metodu ilk kez Glasser ve Strauss (1967) tarafından ortaya konmuş ve birçok araştırmacı tarafından daha da geliştirilerek kullanılmıştır (Strauss ve Gorbin, 1990, 1998).

Genel bir anlatımla, sürekli karşılaştırmalı veri analizi, incelenen verilerin tümevarım kategori şeklinde kodlanması ve aynı zamanda incelenmekte olan verilerle sürekli olarak karşılaştırılması işlemini kapsamaktadır. Bu karşılaştırma işleminde benzerlikler gösteren ya da benzer anlamları kapsayan veriler kalmadığında, yeni bir kategori oluşturulur. Böyle durumlarda oluşturulan bazı kategoriler verileri tam olarak yansıtmadığı gerekçesi ile çıkarılır (Strauss ve Gorbin, 1998). Bu yöntemin veri analizinde birtakım çözümleme araçları bulunmaktadır. Bunlar: açık, birleştirme (aksial) ve seçici kodlamadır. Öğrenci çalışma kağıtlarından elde edilen bulgular, birleştirme kodlamadan yararlanılarak oluşturulmuştur. Yani, her bir etkinlik ve değerlendirme sorularına verilen yanıtlardan aynı ya da benzer olanlar bir araya getirilerek kategoriler oluşturulmuştur. Ayrıca, öğrencilerin verdikleri ilginç ya da o kategoriyi açıklayıcı yanıtlar ise aynen alıntı yapılmıştır.

Ayrıca, ders gözlem formundan ve ders gözlemi sırasında tutulan notlardan faydalanılarak, ders işleme süreci analiz edilmiştir. Ders gözlem formundaki tüm maddeler, ders gözlemi sırasında doldurulmaya çalışılmış, ders sırasında doğrudan doldurulamayan maddeler ise, ders gözleminin hemen sonrasında gözden geçirilerek doldurulmuştur.

BULGULAR

Analiz sonucunda ortaya çıkan bulgular aşağıda ana kısımlar ve örneklerle sunulmaktadır.

Birinci etkinliğe ait bulgular

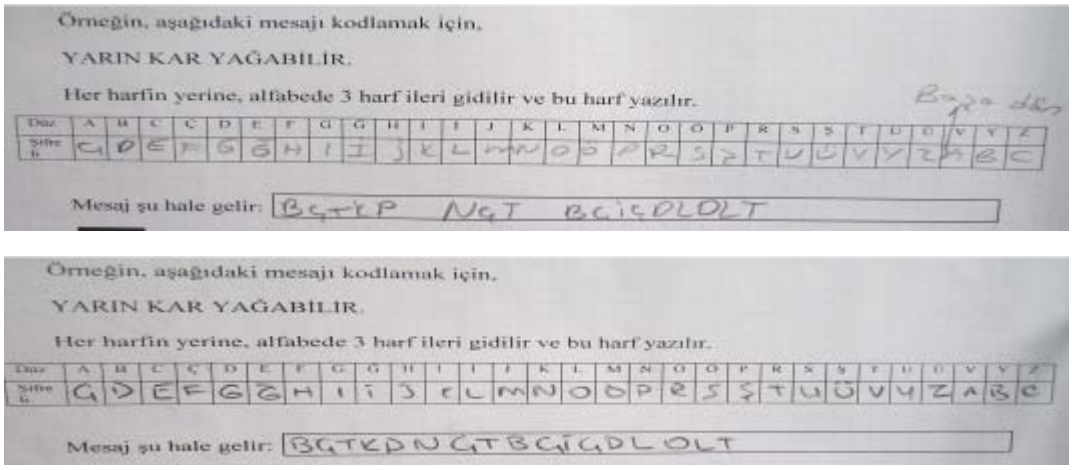
Birinci etkinlikte gerçekleşen öğrenme süreçlerinin incelenmesiyle ilgili bulgular şunlardır:

"Öğretmen: Bugün dersimizde Romalılar tarafından kullanılan mesajları gizlemede kullanılan bir metodu inceleyeceğiz. Bu metot "Sezar Şifrelemesi" olarak adlandırılır. Niçin böyle adlandırılmış olabilir? (Öğrenciler önce cevap veremez.)
Öğretmen: Roma ve Sezar deyince aklınıza ne geliyor?
Bir öğrenci: Sezar onların yöneticisi miydi?
Öğretmen: Evet, Adını Roma imparatoru Julıus Ceasar'dan almıştır.(Bazı öğrencilerden mırıldanmalar geldi: Evet, Sezar. Saçında zeytin yapraklı.)
Öğretmen: Peki, şifreli cümleler nerde işimize yarayabilir?
Bir öğrenci: Derste arkadaşımıza gizli bir şey söylemek istediğimizde.
Bir öğrenci: Bilgisayarda msn, mail gibi adreslerimde.
Bir öğrenci: Cep telefonumdan kısa mesaj atarken.
Öğretmen:(Parmak kaldıran her öğrencinin cevabını başıyla onaylar)Evet, güzel, başka fikri olan?
Bir öğrenci: Gizli telefon konuşmalarında.
Bir öğrenci: Askeriyede parola gibi. Kemal Sunal filminde de vardı. Parolayı söylemeyince vurmuştu(Öğrenciler ve öğretmen güler)."

Matematik programının başarı ile uygulanması için matematik bilgilerinin, hem gerçek hayatla her diğer derslerde öğrenilenlerle ilişkilendirilmesine önem verilmelidir (MEB, 2005). Diyaloglarda görüldüğü gibi öğretmen derse öğrencileri düşünmeye sevkedecek, ilgilerini çekebilecek bir soruyla başlamıştır. Böylece, şifreleme günlük hayatla ilişkilendirilmeye çalışılmıştır. Ayrıca, Sezar ismi genellikle sosyal bilgiler derslerinde ve savaşlarla ilgili kullanılmaktadır. Sezar isminden sonra öğrencilerden biri "Sezar'ın matematiğe yardımcı olması çok ilginç" demiştir. Buradan, konuyla ilgili tartışmalar yapmanın, matematiğe katkısı olan kişileri anlatmanın öğrencilerin derse ilgisini çekmede etkili olduğu söylenebilir.

Öğretmenin şifreleme, şifreleme anahtarı, deşifre etme ve Sezar şifrelemesinden bahsetmesinin ardından, çalışma kağıdında yer alan tabloya Sezar şifrelemesine göre yerleştirilecek harflerin bulunması istenmiştir. Tabloyu bireysel doldururken öğrencilerden "Y'den sonra başa mı geleceğiz?" gibi sorular gelmiştir. Öğretmen soruyu direk cevaplamamış diğer öğrencilere sormuştur. Etkinlik sonunda, öğrencilerden bazıları "… harfler 3 kaydırılsa da sıralı gidiyor…"şeklinde genellemelerde bulmuştur. Şifrelemeyle tanışalım etkinliği sonucunda tüm öğrenciler Türk alfabesini Sezar şifrelemesine göre düzenlemiş ve verilen cümleyi Sezar şifrelemesiyle şifreleyebilmiştir.

Şekil 1. Herhangi iki öğrencinin Sezar şifrelemesi cevapları.



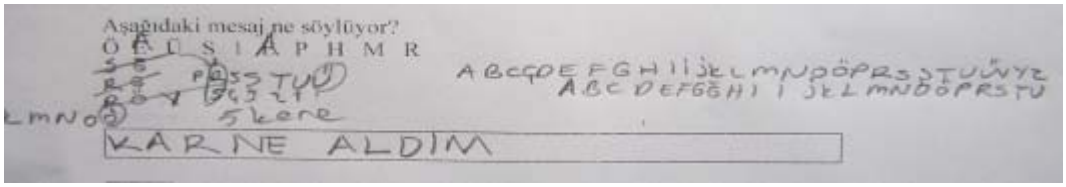
Ders gözlem raporlarına göre, öğretmen ders işleme sürecinde soru yanıt, sınıf tartışması, gösterip yaptırma, düz anlatım yöntemlerini kullanmış, öğrencileri düşünmeye sevk eden sorular sormuş, öğrencilerin matematiğin soyut dilini günlük hayatla bağdaştırmalarını sağlamaya çalışmıştır.

İkinci etkinliğe ait bulgular

İkinci etkinliğe, öğrencilerden "ÖEÜSIEPHMR" cümlesini deşifre etmeleri istenerek başlanmıştır. Öğrenciler harfleri 3 öteleyerek cümleyi deşifre edememişlerdir. Öğretmen öğrencilere "…acaba bu şifreli harfleri 3 öteleme dışında nasıl deşifre edebiliriz?" sorusunu yöneltmiş ve grup arkadaşıyla tartışmalarını istemiştir. Bazı öğrencilerin harfleri sırayla 4 ve 5 defa öteledikleri, bazılarının fikir yürütemedikleri ve bu öğrencilere öğretmenin "…farklı öteleme kullanılmış olabilir mi?" sorusunu yönelterek ipucu verdiği belirlenmiştir.

"Öğretmen: Farklı bir Sezar şifrelemesi nasıl tasarlayabiliriz?
Bir öğrenci: Harfler 4 kaydırılsa da sıralı gidiyor.
Öğretmen: Hadi bakalım, daha çok cevap duymak istiyorum.
Bir öğrenci: Sonsuz kaydırma yapabiliriz, ama 29 kaydırırsak aynı alfabe olur.
Öğretmen: Evet, çok güzel bir cevap. Arkadaşınız 29 harfin kaydırılmasından sonra tekrar eden ilişkiyi de görmüş.
Bir öğrenci: Harfler 28 şekilde kayabilir.
Öğretmen: Niçin 28?
Öğrenci: …(Sessiz, düşünür).
Öğretmen: Cevaplarınızın sebebini açıklayabilmeniz için biraz düşünün. Ben bir öğrenci olup size sebep soracağım.
Bir öğrenci: Harfler 29 şekilde kaydırılabilir.
Öğretmen: Niçin 29 şekilde?
Öğrenci: Çünkü, Z'den sonra baştan yazacağız.
Bir öğrenci: 3 ileri 2 geri gidilebilir.

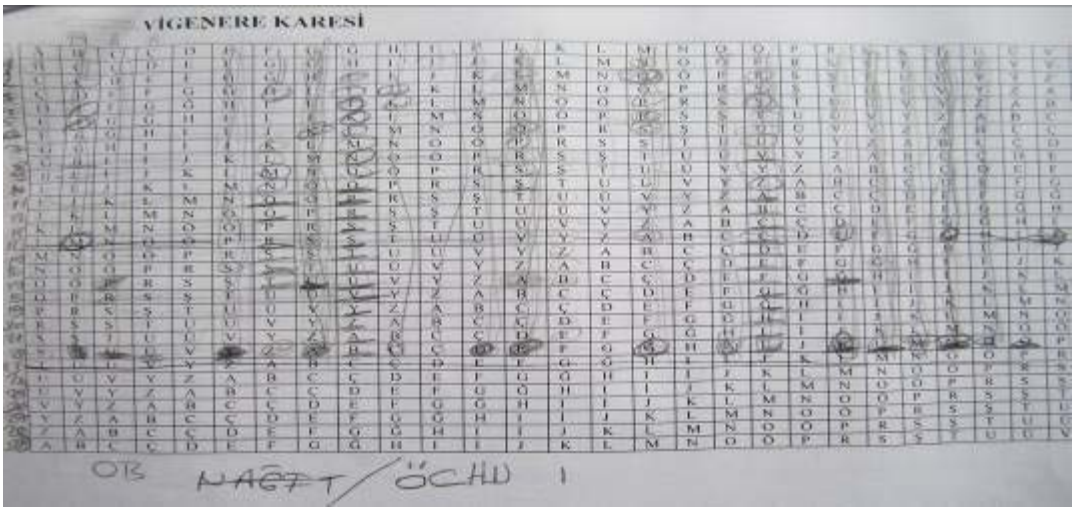
Şekil 2. Herhangi bir öğrencinin yerine koyma şifrelemesi cevabı.



Yukarıdaki diyalogda, öğrencilerden farklı şifreleme stratejileri istendiği görülmektedir. Böylece, öğrencilerin farklı stratejiler üzerinde düşünmeleri, sebep-sonuç ilişkisini kurabilmeleri ve akıl yürütme becerilerinin geliştirilmesi gerçekleşebilir.

Dersin daha sonraki safhasında öğrenciler çalışma kağıtlarındaki Türkçe'ye uyarlanan Vigenere karesini incelediler. Öğrencilerden tüm ötelemelerin yer aldığı bu kare yardımıyla şifreli bir mesajı çiftler halinde çözmeleri istendi. Yapılan etkinlikler incelendiğinde öğrencilerin Vigenere karesini anlamakta güçlük çektikleri ve anlamak için grup arkadaşıyla diyalog kurdukları belirlenmiştir. Öğretmen öğrencilere "…Vigenere karesindeki harfler nasıl dizilmişler?, …ilk satırın karşısına gelen harfler nasıl bir sıra izliyor?, …daha önce yaptığınız harf ötelemeleriyle Vigenere karesinin ilişkisi var mı?" gibi sorular sorarak, öğrencilerin Vigenere karesini anlamalarına rehberlik etmiştir. Etkinlik gerçekleştirildikten sonra öğrencilerin deşifre yöntemleri tartışılmıştır. Öğrencilerden biri "…şifreyi çözerken en çok kullanılan harfi bulup ona baktım. Harfin ünlü olabileceğini düşündüm. Ona göre kaydırmaya baktım." demiştir. Bu öğrenin, ötelemeden farklı bir strateji geliştirdiği söylenebilir.

Şekil 3. Herhangi bir öğrencinin çalışma yaprağındaki Vigenere karesi ve deşifre işlemi.



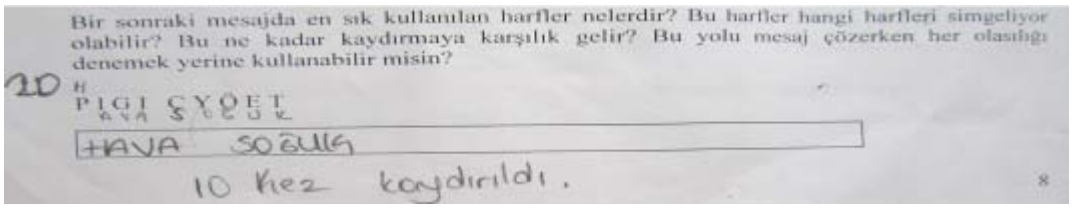
Etkinliklerde öğrencilerden tablolar kullanmaları, tablodan çıkarımda bulunmaları ve bu çıkarımlarını savunmaları istenildiği görülmektedir. Ayrıca, çözüme ulaşılamadığı noktalarda öğretmen cevabı vermek yerine öğrencileri grup arkadaşıyla tartışmaya yöneltmiştir.

Farklı miktarlarda ötelemelerin kullanıldığı cümleleri deşifre ederken yaşanabilecek güçlüklerin neler olduğu sorulduğunda, öğrenciler …" Çok fazla zaman alır. Acil işleri yapamayabiliriz. Kafa karıştırıcı. Hepsini denemek çok sıkıcı." şeklinde görüş belirtmişlerdir.

Öğrenciler Vigenere Karesiyle ilgili, "Önce anlamadım ama arkadaşımla kaydırmaları paylaşınca çok kolay çözdük. Şifreyi çözmemi kolaylaştırdı. Yine de çok vaktimi alıyor. 29 kaydırma olduğu için 15. kaydırmadan bakmaya başladım." şeklinde görüş belirtmişlerdir. Bu bulgulardan öğrencilerin bir problemle karşılaştıklarında yani deşifre etmek için değişik stratejiler geliştirmeye başladıkları söylenebilir. Ayrıca, bu çalışmada öğrencilerin grup arkadaşıyla yardımlaşarak daha hızlı deşifre etmeye çalıştıkları belirlenmiştir.

Daha sonraki uygulamada, deşifre ederken sesli harflerin sessiz harflerle olan ilişkilerinden nasıl faydalanılabileceği üzerine fikir yürütülmüştür. Öğrencilerden, çalışma kağıtlarındaki deşifre edilmesi istenen cümlenin üzerinde yer alan sorulardan ipucu almaları istenmiştir.

Şekil 4. Herhangi bir öğrencinin harf frekansından bahsedilen şifreyi deşifre cevabı.



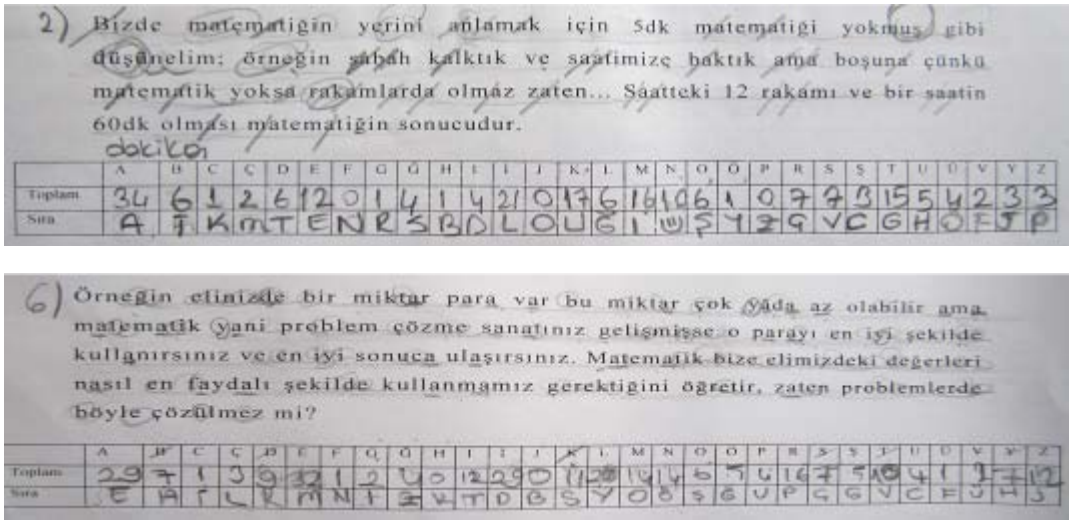
Öğrenciler deşifre için çalışırken öğretmen soruları kendi kendine sorar gibi yüksek sesle söylemiştir: " Bu mesajda en çok kullanılan harfler nelerdir? Bu harfler hangi harfleri simgeliyor olabilir? Bu ne kadar kaydırmaya karşılık gelebilir? Bu mesajı çözerken 29 kaydırma olasılığını da düşünmem gerekli mi?". Üstbiliş becerilerinin gelişimi için sesli düşünme önemlidir. Öğretmenin burada sesli düşünerek öğrencilere model olduğu görülmüştür.

"Öğretmen: Nasıl deşifre ettiğini açıklamak isteyen var mı?
Bir öğrenci: I harfi ipucu veriyor. Sanki A olabilir.
Öğretmen: Niçin A?
Öğrenci: (Kısa bir süre düşünür) Çünkü A çok kullanılır.
Öğretmen: Güzel. Şimdiye kadar öğrendiğimiz yöntemlerden farklı bir cevap. Başka isimleri de dinlemek istiyorum!
Bir öğrenci: En çok tekrarlayan aynı harfe ve aradaki harflere bakıp ünlü mü ünsüz mü düşündüm.
Öğretmen: Çok güzel, yine farklı bir cevap. Pekala herkes düşünüyor: Sizce deşifre etmede sesli ve sessiz harflerin ilişkisinden yararlanabilir miyiz?

Öğrenciler: Evet.
Öğretmen: Peki nasıl?
Bir öğrenci: Kelimelerde bir sesli bir sessiz vardır.
Bir öğrenci: Tren gibi kelimelerde iki sessiz de yan yana ama bu kelimeler az.
Bir öğrenci: Bence sessiz harfler daha çok kullanılır.
Öğretmen: Bu söylediğini arkadaşlarına nasıl ispatlarsın? (Öğrenci cevap veremez, düşünür.)
Öğretmen: Tüm verilen cevapları düşünürsek, cümleleri deşifre etmek için kullanabileceğimiz bir yol da bazı harflerin diğerlerinden daha sık kullanılmaları olabilir mi?
Bir öğrenci: Çarkıfelek yarışmasında da hep benzer harfler söyleniyor.
Öğretmen: Örneğin?
Öğrenci: A ve R gibi.
Öğretmen: Peki o zaman Türkçe'de en sık kullanılan harfleri nasıl bulabiliriz? (Öğrenciler bir süre sessiz kalır, cevap gelmez. Öğretmen çeşitli paragrafların ve paragrafta kullanılan harf frekanslarını belirlemeye yönelik kullanılacak tabloların yer aldığı çalışma kağıdını dağıtır.).
Öğretmen: Aklımıza bir şey gelmiyor mu? O zaman hadi çalışma kağıtlarımıza bakalım.".

Diyaloglarda görüldüğü gibi etkinlikler ilerledikçe öğrencilerde deşifre etmeyle ilgili farklı bakış açıları oluşmaya başlamıştır. Öğrencilerin harf frekansını ve kelime desenlerini deşifre etmede kullanmayı sezdikleri söylenebilir. Etkinlik sürecinde, öğrencilerin çift olarak çalıştığı, birinin paragraflardaki harfleri sayarken diğerinin kaydettiği görülmüştür.

Şekil 5. Herhangi iki öğrencinin harf frekansı tabloları.

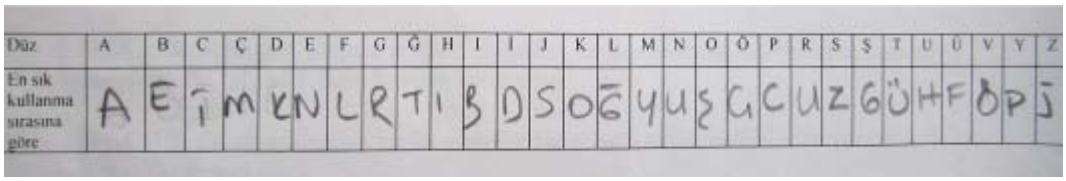


Her grubun en sık kullanılan 4 harfi belirlemesi istenmiş, gelen cevapların niçin farklılıklar gösterdiği tartışılmıştır. Bazı öğrenci cevaplarının "… Paragraflardaki kelime sayıları farklı. Paragrafın uzunluğuna bağlı. Her paragrafta değişik kelimeler var." şeklinde olduğu belirlenmiştir. Tüm grupların cevapları tahtaya yazılmış ve Türkçe'de en çok kullanılan ilk 4 harfin A,İ,E,M olduğu kararlaştırılmıştır. Öğretmen tarafından öğrencilere "Türkçe metinlerde harf frekansı" ödevi verilmiştir. Öğrencilerden sınıfta yapılan çalışmanın benzer bir çalışmasını evde daha uzun hikaye tarzı anlatımlar üzerinde yaparak, harf frekanslarını belirlemeleri istenmiştir.

Üçüncü etkinliğe ait bulgular

Öğrencilere verilen ödevden yararlanarak harf frekanslarına göre Türk Alfabesi yeniden düzenlenmiştir.

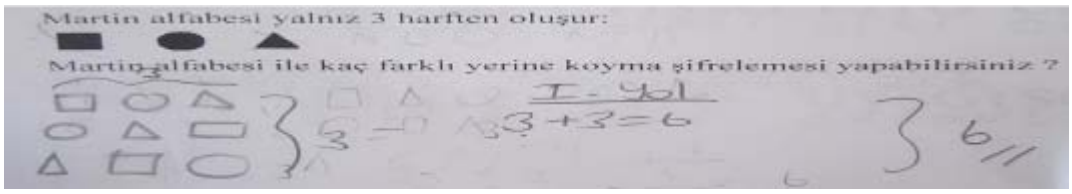
Şekil 6. Harf frekanslarına göre düzenlenmiş alfabe



Daha sonra, yerine koymalı şifrelemede alfabedeki her bir harfin rastgele bir başka harf ile yer değiştirmesi mantığından yola çıkılarak permütasyon konusu gösterilmiştir. Permütasyon sonucu oluşabilecek anahtar sayısını göstermede kolaylık olması amacıyla faktöriyel sembolü açıklanmıştır.

"Öğretmen: Şimdi de sadece 3 tane geometrik şekilden oluşan Martin alfabesiyle tanışacağız. (Öğretmen tahtaya kare, daire ve üçgen çizer.) İşte Martin alfabesinin harfleri. Bu alfabeyi kullanarak ve her harfin yerini rastgele başka bir harfle değiştirerek kaç farklı şifreleme anahtarı oluşturabiliriz? Bulduğunuz her şeyi çalışma yapraklarına da yazın lütfen. (Öğretmen öğrencilere müdahale etmeden birkaç dakika bekler).
Öğretmen: Cevabı bulan var mı?
Bir öğrenci: 6 şekilde.
Öğretmen: Bulduklarını tahtada gösterir misin?
Öğrenci: Şekillerin sırayla yerlerini değiştirdim.(Anlattığı gibi tahtaya şekiller çizer) 3 tane satırda şekil, 3 tane sütunda şekil var. 3+3=6 şekilde şifreleme yaparım.

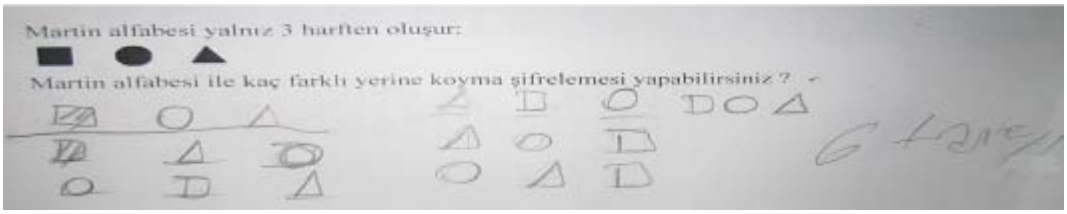
Şekil 7. Öğrencinin çalışma yaprağına vermiş olduğu cevap.



Öğretmen: (Sınıfa sorar) Arkadaşınızın cevabı doğru mu?
Bir öğrenci: Kare baştayken yanına üçgen de gelebilir.
Öğretmen: (Tahtadaki öğrenciye söyler). Arkadaşının söylediği şekilde şifreleme yapabilir misin?
Öğrenci: Aaa…Evet, o da var. (Kare, üçgen, daire çizer).
Öğretmen: Bütün sıralaman bitti mi? (Diğer öğrenciler parmak kaldırır).
Öğrenci: O zaman dairenin yanı da değişir. (Daire, kare, üçgen çizer. Öğretmen sınıftan başka bir öğrenciye söz verir).
Bir öğrenci: Üçgenin yanındakiler de değişir. Mesela, üçgen, daire, kare olur.(Tahtadaki öğrenci arkadaşlarının söylediklerini tahtaya çizer.)

Bir öğrenci: Örüntü gibi düşündüm. Önce kareyi başa alır yanındakileri değiştiririm, sonra daireyi ve üçgensel bölgeyi başa alır yanındakileri değiştiririm.

Şekil 8. Öğrencinin çalışma yaprağına vermiş olduğu cevap.

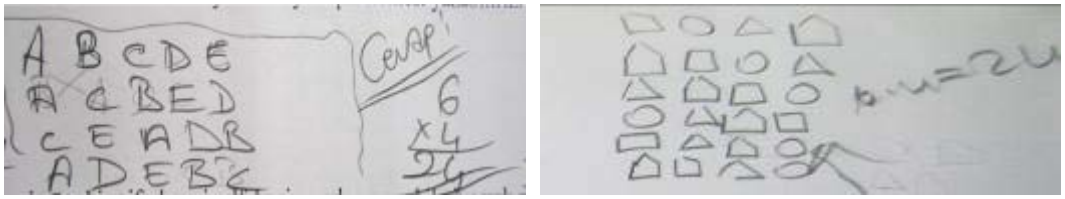


Öğretmen: Tahtada başka yer değiştirme yapabilir miyiz?
Bir öğrenci: Aynıları oluyor.
Öğretmen: Toplam kaç farklı şifreleme anahtarı bulduk?
Sınıf: Altı."

Şekil 9. Herhangi bir öğrencinin çalışma yaprağındaki cevap.

Etkinliğin devamında Martin alfabesine bir beşgen şekli eklenerek oluşan Venusian alfabesindeki harflerle kaç farklı şifreleme anahtarı oluşturulabileceği tartışılmıştır. Öğrencilerden 8 tanesi şekil çizerek cevaba ulaşmıştır. Öğrenciler cevaplarını yukarıda verilen diyaloğa benzer şekilde açıklarken bir öğrenci, "Harflerden birini sabit tutunca yanındakiler 6 şekilde değişiyor. 4 harf var, o zaman 6.4=24 şekilde şifreleme yapabilirim." demiştir.

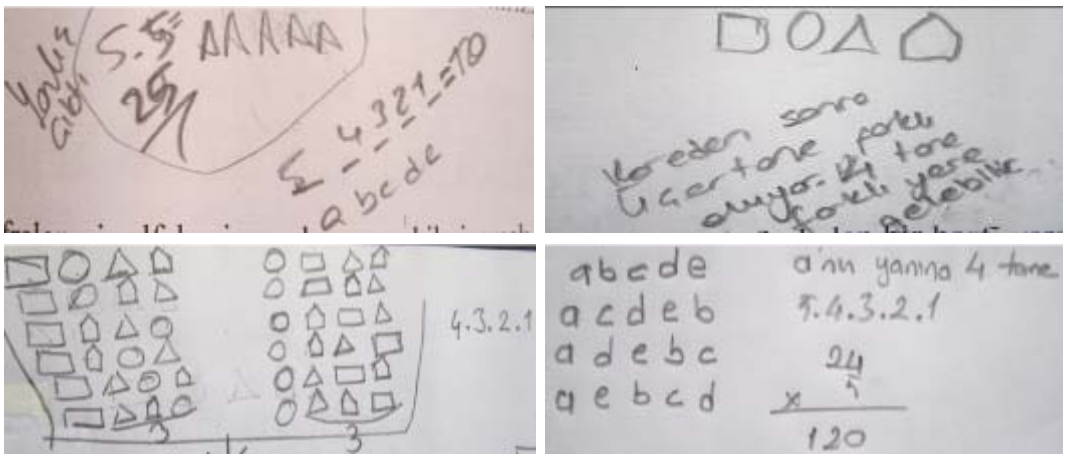
Şekil 10. Herhangi iki öğrencinin çalışma yaprağına vermiş olduğu cevaplar.



Öğretmen şekil çizmekten daha farklı nasıl bir yolla sıralama yapılabileceğini sınıfa sorar ve cevapları üzerinde tartışılır. Öğretmen, 4 harf için harflerin yan yana dizilme seçeneklerini öğrenci cevaplarını da dinleyerek tahtaya yazar, "İlk başa 4 harf yazarsak yanına 3 harfimiz kalır. Bir harf daha kullanırsak üçüncü sıraya 2 harf kalır. Ve en sona sadece 1 harfimiz kaldı. Tüm durumları çarpalım ve sonuç 24 farklı durum.". Daha sonra 5 harfli bir alfabe için, 29 harfli Türk alfabesi için ve n harfli bir alfabe için etkinlik tekrarlanır. Öğretmenin, öğrencilerin 6. sınıfta öğrendikleri saymanın temel ilkelerinden ve yerine koyma şifrelemesinin genel

uygulamalarından yararlanarak permütasyon konusunu açıkladığı görülmüştür. Öğrencilerin permütasyon işlemlerini kullanarak cevaba ulaştıkları görülmüştür.

Şekil 11. Herhangi dört öğrencinin çalışma kağıtlarındaki cevaplar.



Alfabedeki harflerin artmasıyla gerçekleştirilen sıralamanın olumsuz yönlerinin öğrencilere sorulması durumunda, cevaplar "Sayı çok büyük ve uzun sürüyor. Cevabı bulamıyorum çünkü çok büyük çıkıyor. 29.28 yazdıktan sonra araya …… koyarım." şeklinde olmuştur. Öğretmen açıklamaları yaparken öğrencilere sorular yöneltip, ortaya çıkan durumları tahtaya yazarak öğrencilere geri bildirim vermiştir. Öğretmen, tahtadaki örneklerden yararlanarak aşağıdaki diyalogları gerçekleştirmiştir:

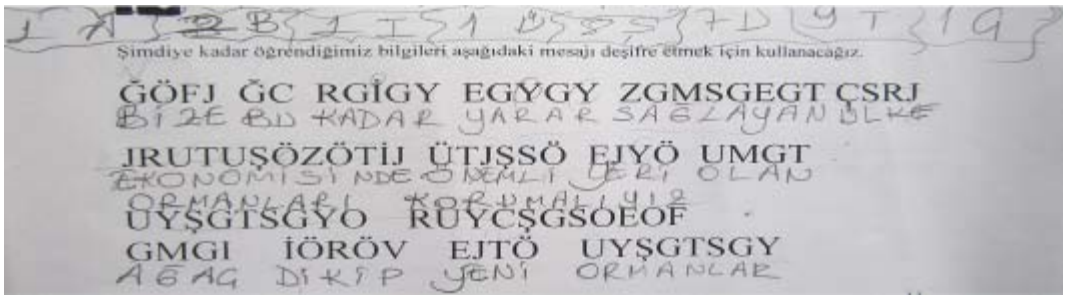
"Öğretmen: 1'den 5 'e kadar olan ardışık sayıların çarpımını kısaca 5! şeklinde göstersem ve bunu 5 faktöriyel diye okusam, 1'den 29'a kadar olan çarpımları nasıl ifade ederim?
Öğrenciler: 29 faktöriyel (Öğretmen tahtaya 29! yazar.).
Öğretmen: Peki 1'den n'ye kadar olan çarpımları?
Öğrenciler: n faktöriyel (Öğretmen tahtaya n! yazar.).
Öğretmen: Peki 1'den x'e kadar olan çarpımları?
Öğrenciler: x faktöriyel (Öğretmen tahtaya x! yazar.)."

Öğretmenin tahtada faktöriyel sembolünü renkli tebeşirle vurguladığı görülmüştür. Öğretmen 1'den belirli bir sayıya kadar olan sayıların çarpımlarını göstermede faktöriyel sembolünün kullanıldığını açıklar. Öğretmen konunun iyi anlaşılması için, harfleri sıralama işlemine permütasyon denildiğini söyler. Açıklamalardan sonra ise öğrencilerin tamamı öğretmenin sözel olarak sorduğu "6 arkadaş yan yana kaç farklı şekilde oturabilir?, 10 kişi yan yana kaç farklı şekilde halay çekebilir?" gibi sorulara doğru cevap vermiştir.

Daha sonra, öğrencileri tüm öğrendikleri stratejileri gözden geçirip en uygun stratejiyi seçmeye sevk etmek amacıyla şifrelenmiş uzun bir parça cümle verilip deşifre etmeleri istenmiştir. Öğrencilere hangi yolu kullandıkları sorulduğunda öğrenciler, "Vigenere karesi en

zevkli olanı. 7. kaydırmada çıktı. En sık kullanılan harfe göre gittim. Frekansa göre olan alfabeye göre denedim. En çok kullanılan harfin A, sonra E olmasına baktım. Anlamlı kelimeler buldum." gibi cevaplar vermiştir. Öğrencilerin farklı stratejilerle deşifre ettikleri, daha önce öğrenilen yolları kullanabildikleri görülmüştür.

Şekil 12. Herhangi bir öğrencinin çalışma kağıdındaki deşifre cevabı.



Çalışma kağıdı sonuna "Bu çalışma hakkındaki düşüncelerim" bölümü eklenerek, bu kısma öğrencilerden çalışma sonunda şifreleme, faktöriyel ve permütasyon etkinlikleriyle ilgili görüşlerini yazmaları istenmiştir. Öğrenci görüşlerinden bazıları aşağıda verilmiştir:

"Önce şifreleri bulamam diye korktum ama sonra korkmadım çünkü arkadaşım da vardı. Ders çok zevkliydi.
Eğlenerek ve çok düşünerek ders işledik ama bir daha faktöriyel işaretini hiç unutmam.
Daha önce kitaplardan ünlem işareti gibi faktöriyel işareti görmüştüm ama işlemleri anlamadım. Ama şimdi anladım ve ders çok eğlenceliydi.
Sanki oyun gibi matematik işledik. Ben de arkadaşlarımla şifreli konuşabilirim artık. Şekilleri sıralamayı kolayca ve hızlı yapabilirim artık."

Öğrenci görüşlerinden yola çıkarak, öğrencilerin şifrelemeyi öğrendikleri, faktöriyel işaretini anlamlı yapılandırdıkları, dersin zevkle ve oyun gibi işlendiği ve öğrencilerin korkularının giderildiği söylenebilir.

SONUÇ ve TARTIŞMA

Bu araştırmada, ilköğretim yedinci sınıf faktöriyel ve permütasyon konusunun öğretiminde kullanılabilecek şifreleme etkinlikleri tasarlanarak, bu etkinliklerin kullanıldığı sınıf ortamında gerçekleşen öğretme-öğrenme süreçleri analiz edilmiştir.

Gelişen teknolojinin ihtiyaçlarına uyum ve matematiğin günlük hayatta kullanımının gösterilmesi için öğrenciler Sezar ve yerine koyma şifrelemesi ile tanıştırılmıştır. Araştırma bulgularına göre, öğrencilerin kendilerine verilen ifadeleri Sezar şifrelemesini kullanarak şifreleyebildikleri saptanmıştır. Araştırma sonucunda, öğrencilerin Sezar şifrelemesinden yola çıkarak yerine koyma şifrelemesini öğrendikleri, çeşitli şifreleme ve deşifre işlemlerini gerçekleştirdikleri belirlenmiştir. Şifreleme ve deşifre işlemleri sürecinde öğrencilerin

Vigenere karesini kullandıkları ve harf frekanslarından yararlandıkları saptanmıştır. Ayrıca, öğrencilerin şifrelemenin günlük hayatta kullanımıyla ilgili fikir sahibi oldukları söylenebilir. Literatürdeki benzer araştırmalardaki sonuçlar araştırmanın sonuçlarıyla paralellik göstermektedir. Evered ve Gningue (2001)'in araştırmasında benzer şekilde öğrenciler temel şifreleme ve deşifre teknikleriyle tanıştırılmıştır. Bachman, Ezra ve Norton (2010) çalışmalarında şifrelemenin günlük hayattaki önemine değinerek, öğrencilerin şifreleme ve deşifre yapabilecekleri etkinlikler tasarlamışlardır. Chua (2006), matris öğretiminde öğrencilerine öncelikle Sezar şifrelemesini tanıtmıştır. Yapılan her üç çalışma sonuçlarına göre, etkinlikler yardımıyla şifrelemelerde kullanılabilecek matematiksel kavramların ve işlem becerilerinin kazanıldığı ve deşifre uygulamalarında kullanıldığı belirlenmiştir. Ayrıca, Chua (2006) şifreleme etkinlikleri kullanarak gerçekleştirilen matematik öğretiminin, matematiğin günlük hayatta önemli bir rolü olduğunu göstermede kolaylık sağlayacağını belirtmektedir.

Permütasyon ve faktöriyel, matematik ve günlük hayat arasında bağlantı kurulmasını gerektiren, olasılık gibi konulara temel teşkil eden konulardır. Araştırmada, öğretmenin yerine koyma şifrelemesi uygulamalarını aşamalı olarak öğrencilere uygulattığı saptanmıştır. Bu uygulama süreçlerinde, öğrencilerin şifreleme ile permütasyon arasında sebep-sonuç ilişkisi kurmalarına yardımcı olduğu belirlenmiştir. Bu şekilde, permütasyon ve faktöriyel konularının buluş yoluyla öğrencilere kazandırıldığı saptanmıştır. Konu öğretiminde şifreleme etkinlikleri kullanımının anlamlı öğrenmeler gerçekleşmesine yardımcı olacağı düşünülmektedir. Yapılan benzer çalışmalarda da matematik konularının öğretiminde şifreleme etkinlikleri kullanılmıştır (Chua, 2006, 2008; Güler, 2007; Hall, 2003; Özdemir ve Güler, 2008; Saygı ve Umay, 2010). Hall (2003) şifreleme ve deşifre uygulamalarının öğrencilerin modüler aritmetik konusunu öğrenmelerini kolaylaştırdığını ifade etmektedir. Ayrıca, şifrelemenin motivasyonda etkili olduğunu belirtmektedir.

Güler (2007) ve Özdemir ve Güler (2008) araştırmalarında, ilköğretim 8. sınıflarda modüler aritmetik konusunun öğretiminde şifreleme aktiviteleri kullanımının öğrenci başarısı ve kalıcılık düzeyine etkisini incelemiştir. Bu araştırmanın bulguları, modüler aritmetik konusunun öğretiminde şifreleme aktiviteleri kullanılmasının matematik başarısını olumlu yönde etkilediğini göstermektedir. Ayrıca, öğrencilerin matematik tutumlarının da olumlu geliştiği ifade edilmiştir.

Yapılandırmacı anlayışın temel alındığı yeni programda öğrenci merkezli etkinlikler büyük yer tutmaktadır. Araştırmada etkinliklerin uygulanması sürecinde öğrencilerin yaparak ve yaşayarak öğrendikleri, tartışma durumları yaratılarak eleştirel ve sorgulayıcı ortamların oluşturulduğu, soru cevap, gösterip yaptırma, işbirliğine dayalı öğrenme gibi yapısalcı anlayışa uygun yöntem ve tekniklerin kullanıldığı belirlenmiştir. Bu sonuç, etkinlik temelli öğretim gerçekleştirilen araştırma sonuçlarıyla tutarlılık göstermektedir (Arı, Çavuş, Sağlık, 2010; Bachman, Ezra ve Norton, 2010; Evered ve Gningue, 2001; Hiçcan, 2008; Palabıyık, 2010;

Sağlık, 2007; Şengül ve Ekinözü, 2006, 2007). Yapılan bu çalışmalarda ders işleme sürecinde etkinlikler kullanılarak öğrencilerin aktif katılımları sağlanmıştır. Kaur (2008), üniversite öğrencilerinin matematiğe ilgisini arttırmak, onları araştırmaya sevk etmek ve motive etmek için şifrelemenin öğretimsel bir araç olarak kullanıldığı dersler planlamıştır. Derslerde sınıf tartışması, grup çalışması ve araştırma ödevleri yer almaktadır. Şifreleme tekniklerini tartışan öğrenciler, şifrelemelerde kullanılan matematik konu ve kavramlarını da derinlemesine araştırıp öğrenmişlerdir. Bu durum, doğal olarak öğrencilerin derse ilgilerini ve motivasyonlarını arttırmıştır. Evered ve Gningue'nun (2001) etkinlik temelli çalışmaları sonucunda öğrencilerin eleştirel düşünme becerisi kazanmaları sağlanmıştır.

Ayrıca, etkinliklerin uygulama sürecinin öğrencilerin iletişim becerilerinin gelişmesini de olumlu etkilediği belirlenmiştir. Grup çalışmasındaki olumlu etkileşim sonucunda etkinliklerin iyi seviyede gerçekleştiği söylenebilir. Kaur (2008) de çalışmasında grup çalışması ve iletişime önem vermiştir. Tüm bu olumlu sınıf ortamının öğrenci başarısını arttırmada önemli bir rol oynayacağı söylenebilir.

Araştırma sürecinde öğretmenin sürekli sorular sorduğu, sınıf tartışmalarına zemin hazırladığı, işbirliğine dayalı çalışma için öğrencileri yönlendirdiği belirlenmiştir. Öğretmenin, şifreleri ve problemleri direk çözmek yerine ipucu verdiği, öğrencilerin genel sonuçlara varmalarına yardımcı olduğu saptanmıştır. Bu sonuç, Myerscough ve diğerlerinin (1996) araştırma sonuçları ile paralellik göstermektedir. Myerscough ve diğerlerinin (1996) çalışmalarında da öğretmenin öğrencilerin şifreyi çözmede zorlandıkları anlarda ipucu vererek onları yönlendirdiği saptanmıştır. Araştırmacılar bazı sınıfların şifreyi çözmede zorlandıklarını, bazılarının öğretmen ipucu vermeden şifre hakkında yorum yapmadıklarını fakat birçoğunun şifreyi çözmede inatçı ve başarılı olduğunu ifade etmektedir.

ÖNERİLER

Yapılan çalışmada tasarlanan şifreleme etkinlikleri daha kalabalık sınıf ortamlarında uygulanarak sonuçları değerlendirilebilir. Faktöriyel ve permütasyon konusunun öğretilmesinde şifreleme etkinliklerinin kullanılması sonucu öğrencilerin matematik dersine karşı tutumları ve akademik başarılarını ölçen daha ayrıntılı çalışmalar gerçekleştirilebilir. Öğrencilerin farklı yetenek ve ilgilere sahip oldukları göz önüne alınarak, etkinlik uygulamaları sonucu değerlendirme ölçekleri hazırlanabilir. Şifrelemenin farklı matematik konularında kullanımını gerektiren etkinliklerin tasarlandığı, etkinlikler ile öğrenci başarısı arasındaki ilişkilerin, öğretmen görüşlerinin incelendiği daha kapsamlı araştırmalara ülkemizde de yer verilmelidir.

Bilgisayar ve iletişim teknolojilerindeki gelişmelerin oluşturduğu sayısal toplumun gereksinimi olan insanların yetiştirilmesi için ilköğretim matematik öğretim programlarına şifreleme konusu eklenebilir. Öğretmenler tarafından şifrelemenin günlük hayatta

kullanımıyla ilgili öğrencilere verilebilecek performans ve proje görevleri geliştirilebilir. Gerver ve Sgroi (2003)'nin de belirttiği gibi, öğrenciyi aktif kılacak öğretme yaklaşımını gerçekten uygulamak isteyen bir öğretmen, buna uygun ders planını kendisi de yazabilir. Gerver ve Sgroi (2003)'nin de öneri olarak sunduğu gibi, her öğretmen bir yıl boyunca altı etkinlik geliştirse, yılsonunda zümrenin elinde iyi bir etkinlik ve ders planı arşivi oluşacak ve bu arşiv her yıl daha da genişletilebilecektir.

KAYNAKÇA

Altun, M. (2004). *Matematik öğretimi* (3. Baskı). İstanbul: Alfa Basın Yayım Dağıtım.

Arı, K., Çavuş, H. ve Sağlık, N. (2010). İlköğretim 6. sınıflarda geometrik kavramların öğretiminde etkinlik temelli öğrenimin öğrenci başarısına etkisi. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi*, 27, 99-112.

Arslan, E.N. (1994). *Matematik Öğretiminde Programlı Öğretim Yönteminin Etkililiği.* Yayımlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Soysal Bilimler Enstitüsü, Eskişehir.

Bachman, D.J.; Ezra, A. ve Norton, A.H. (2010). Chocolate key cryptography. (ERIC Document Reproduction Service No. EJ898327).

Başar, M.S. (2004). *Yer değiştirme Esaslı ve Rasgele Anahtarlı Yeni Bir Şifreleme Algoritması.* Yayımlanmamış Doktora Tezi, Atatürk Üniversitesi Soysal Bilimler Enstitüsü, Erzurum.

Baykul, Y. (2005). *İlköğretimde matematik öğretimi (1-5. sınıflar).* Ankara: PegemA Yayıncılık.

Boyacıoğlu, H., Erduran, A. ve Alkan, H. (1996). *Permütasyon, kombinasyon ve olasılık öğretiminde rastlanan güçlüklerin giderilmesi.* II. Ulusal Eğitim Sempozyumu, İstanbul.

Buluş, H.N. (2006). *Temel Şifreleme Algoritmaları ve Kriptanalizlerinin İncelenmesi*. Yayımlanmamış Yüksek Lisans Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Bulut, S. (1994). *The Effects of Different Teahing Methods Gender On Probability Achievement And Attitudes toward Probability*. Yayımlanmamış Doktora Tezi, Orta Doğu Teknik Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Chua, B.L. (2006). Harry potter and the cryptography with matrices. *Australian Mathematics Teacher, 62(3),* 25-27.

Chua, B.L. (2008). Harry potter and the coding of secrets. *Mathematics Teaching in the Middle School*, *14(2),* 114-121.

Cooperstein, S.E. ve Kocevar-Weidinger, E. (2004). Beyond active learning: A construstivist approach to learning. *Reference Services Review*, *32 (2),* 141-148.

Çalışkan, E.M. (2004). *Şifreleme Algoritmalarının Performans-Kripto Analizleri ve Eğitimde Kullanılması*. Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Eğitim Bilimleri Enstitüsü, İstanbul.

Çubuk, Ş. (2004). *Matematik Öğretiminde "Permütasyon ve Olasılık" Konusunun Bilgisayar Destekli Öğretim Materyalleri İle Öğretilmesinin Öğrenci Başarısına Etkisi*. Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Eğitim Bilimleri Enstitüsü, İstanbul.

Demirel, Ö. (2004). *Eğitimde Program Geliştirme* (6.baskı). Ankara: PegemA Yayıncılık.

Ekinözü, İ. (2003). *İlköğretimde Permütasyon ve Olasılık Konusunun Dramatizasyon İle Öğretiminin Başarıya Etkisinin incelenmesi*. Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Eğitim Bilimleri Enstitüsü, İstanbul.

Ercan, Ö.(2008). *Çoklu Zekâ Kuramına Dayalı Öğretim Etkinliklerinin 8. Sınıf Öğrencilerinin Matematik Dersi "Permütasyon ve Olasılık" Ünitesindeki Akademik Başarılarına Etkisi.* Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Evered, L.J. ve Gningue, S. (2001). Developing Mathematical Thinking Using Codes and Ciphers. (ERIC Document Reproduction Service No. EJ670445).

Gerver, R. K. ve Sgroi, R. J. (2003). Creating and using guided-discovery lessons. *Mathematics Teacher*, *96(1),* 6-13.

Güler, E. (2007*). Modüler Aritmetik Konusunun Öğretiminde Şifreleme Aktivitelerinin Matematik Başarısına Etkisi*. Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Eğitim Bilimleri Enstitüsü, İstanbul.

Hall, M. (2003). Calculator cryptography. *Mathematics Teacher*, *96(3),* 210-212.

Hamilton, M. ve Yankosky, B. (2004). The Vigenere Cipher With The TI-83. (ERIC Document Reproduction Service No. EJ720442).

Hiçcan, B. (2008). *5e Öğrenme Döngüsü Modeline Dayalı Öğretim Etkinliklerinin İlköğretim 7. Sınıf Öğrencilerinin Matematik Dersi Birinci Dereceden Bir Bilinmeyenli Denklemler Konusundaki Akademik Başarılarına Etkisi*. Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Jacobsen, T. (1995). A fast method for the cryptanalysis of substitution ciphers. *Cryptologia*, *19(3),* 265-274.

Karaahmetoğlu, O. (2010). *Gizli Anahtarlı Kriptosistemlerin Tasarımında Cebirsel Yapıların Önemi ve Kriptanaliz*. Yayımlanmamış Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Kaur, M. (2008). Cryptography as a pedagogical tool. (ERIC Document Reproduction Service No. EJ810999).

McCartney, M. (2000). Reading writing and some basic arithmetic: Using ambc zpcyigle in the classroom. *Teaching Mathematics and Its Applications, 19(4),*179-182.

McMillan, J.H. ve Schumacher, S. (2001*). Research in Education. A Conceptual Introduction.* **(**Fifth Edition). Addison Wesley Longman.

MEB (2005). *İlköğretim Matematik Dersi Öğretim Programı ve Kılavuzu*. Ankara: Devlet Kitapları Müdürlüğü.

MEB (2007). *Öğretmen Kılavuzu Matematik 7.* İstanbul: Milli Eğitim Basımevi.

Myerscough, D., Ploger, D., McCarthy, L., Hopper, H. ve Fegers, V. (1996). Cryptograpy: Cracking Codes. (ERIC Document Reproduction Service No. EJ538337).

Olkun, S. ve Aydoğdu, T. (2003). Üçüncü uluslararası matematik ve fen araştırması (tımss) nedir? Neyi sorgular? Örnek geometri soruları ve etkinlikler. *İlköğretim Online,* 2(1), 28–35.

Online: <www.cimpt.plymouth.ac.uk/resources/codes/codes_u1_1p.pdf> 23.09.2007 tarihinde erişilmiştir.

Online: <www.purdue.edu/discoverypark/gk12/downloads/Cryptography.pdf> 02.10.2011 tarihinde erişilmiştir.

Özdemir A.Ş. ve Güler E. (2008). *Modüler Aritmetik konusunun öğretiminde şifreleme aktivitelerinin matematik başarısına etkisi*. Uluslararası Eğitim Bilimleri Kongresi, Gazi Mağusa-K.K.T.C. (23-25 Haziran).

Öztürk, G. (2005). *İlköğretim 8. Sınıf Düzeyinde Permütasyon ve Olasılık Ünitesinin Bilgisayar Destekli Tasarımı*. Yayımlanmamış Yüksek Lisans Tezi, Balıkesir Üniversitesi Fen Bilimleri Enstitüsü, Balıkesir.

Palabıyık, U. (2010). *Örüntü Temelli Cebir Öğretiminin Öğrencilerin Cebirsel Düşünme Becerileri Ve Matematiğe Karşı Tutumlarına Etkisi*. Yayımlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi Sosyal Bilimleri Enstitüsü, Ankara.

Sağlık, N. (2007). *Pilot Uygulamaları Yürütülen İlköğretim Matematik Programına Yönelik Etkinliklerin Bazı Geometri Konularının Öğretimi Üzerindeki Etkisi.* Yayımlanmamış Yüksek Lisans Tezi, Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü, Van.

Saygı, E. ve Umay, A. (2010). *Kriptoloji yardımıyla fonksiyon kavramının oluşturulması*. 9. Matematik Sempozyumu, Trabzon (20-22 Ekim).

Singh S. (1999). *Code book; the evolution of secrecy from Mary Queen of Scots to quantum cryptography.* USA: Anchor.

Stallings, W. (1998). *Cryptography and network security:Priciples and practice*. New Jersey: Prentice Hall.

Strauss, A. ve Gorbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques.* London: SAGE.

Strauss, A. ve Gorbin, J. (1998). *Basics of qualitative research: Procedures and techniques for grounded theory*. London: SAGE.

Şengül, S. ve Ekinözü, İ. (2006). Canlandırma yönteminin öğrencilerin matematik tutumuna etkisi. *Kastamonu Eğitim Dergisi*, *14(2),* 517-526.

Şengül, S. ve Ekinözü, İ. (2007). Permütasyon ve olasılık konusunun öğretiminde canlandırma kullanılmasının öğrenci başarısına ve hatırlama düzeyine etkisi. *Kastamonu Eğitim Dergisi*, *15(1),* 251-258.

Temizöz, Y. ve Özgün-Koca, S.A. (2008). Matematik öğretmenlerinin kullandıkları öğretim yöntemleri ve buluş yoluyla öğrenme yaklaşımı konusundaki görüşleri. *Eğitim ve Bilim,* 33(149), 89-103.

Tuncal, T. (2008). *Bilgisayar Güvenliği Üzerine Bir Araştırma ve Şifreleme-Deşifreleme Üzerine Uygulama.* Yayımlanmamış Yüksek Lisans Tezi, Maltepe Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Yazıcı, E. (2002). *Permütasyon ve Olasılık Konusunun Buluş Yoluyla Öğretilmesi.* Yayımlanmamış Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü, Trabzon.

Yıldırm, A. ve Şimşek, H. (2005). *Sosyal Bilimlerde Nitel Araştırma Yöntemi*. Ankara: Seçkin Yayıncılık.