Matematika C

10. osztály

6. modul
Kódoltam

Készítette: Kovács Károlyné

A modul célja	Ismerkedés a kódolási alapismeretekkel. A mindennapi életben gyakran látott kódok megismerése.
Időkeret	3 foglalkozás
Ajánlott korosztály	15–16 évesek (10. osztály)
Modulkapcsolódási pontok	Tágabb környezetben: irodalom Szűkebb környezetben: bármelyik tantárgy, amelyik igényli a tanulók elemzőképességét. Ajánlott megelőző tevékenységek: a százalékszámítás és a kettes számrendszer ismerete, valószínűség, relatív gyakoriság
A képességfejlesztés fókuszai	Számolás, számlálás Mennyiségi következtetés, valószínűségi következtetés Becslés, mérés Szöveges feladat megoldása, probléma megoldás, metakogníció Rendszerezés, kombinativitás Valószínűség, statisztika

AJÁNLÁS

A tanulók a mindennapi életben gyakran találkoznak különböző kódokkal. Az adatok továbbításának három fő problémája van: a biztonság, a titkosság és a tömörség. A biztonság kérdésével a kódelmélet, a titkosságéval a kriptográfia, a tömörséggel az információelmélet foglalkozik.
Ez a modul az első két problémával foglalkozik: a titkossággal és a biztonsággal. A tanulók megismerkednek néhány titkosírási móddal, valamint egy másik ábécével (morze ábécé). A második és harmadik foglalkozáson a biztonság kérdésével foglalkozunk kétfajta kód – az áruk vonalkódjának és a könyvek ISBN számának – megismerésén keresztül. Megismerik a tanulók az ellenőrző jegy szerepét, hibafelismerésének korlátjait. Végül egy csapatok közötti versenyen módjuk nyílik megismerkedni a paritásbittel, és annak alkalmazási módjával is.

TÁMOGATÓ RENDSZER

Simon Singh: *Kódkönyv* (Park Könyvkiadó)
Közös nevezőnk a matematika (Kőszeg 2002)
www.fazekas.hu/matek*
Új matematikai mozaik (Typotex, 2002)
Nemetz Tibor–Wintsche Gergely: *Valószínűségszámítás és statisztika mindenkinek* (Szeged, Polygon, 1999)

* 2007. augusztusában elérhető a honlap

MODULVÁZLAT

	Lépések, tevékenységek	Kiemelt készségek, képességek	Eszközök, mellékletek
I. Kriptográfia			
1.	Átrendezéses és behelyettesítéses kódolás	Analógiás gondolkodás, elemző képesség, figyelem, koncentráció, problémaérzékenység, gondolkodási sebesség, ismeretek rendszerezése, problémamegoldás, kombinatorikus gondolkodás	Eszközök: Csoportonként másolat Az üzenetek c. mellékletből Tanulói munkafüzet: Ábécé a behelyettesítéses kódrendszer kialakításához Melléklet a tanároknak: A kódolt szöveg és megoldása Az üzenetek
2.	Gyakoriság, relatív gyakoriság	Elemző képesség, figyelem, koncentráció	Eszköz: Egy hosszabb szöveg bekezdései

	Lépések, tevékenységek	Kiemelt készségek, képességek	Eszközök, mellékletek
II. Vonalkód			
	Ráhangolódás	Problémaérzékenység, gondolkodási sebesség	Tanulói munkafüzet: A morzeábécé
1.	A morzeábécé	Problémaérzékenység, gondolkodási sebesség, egymásra figyelés, ismeretek rendszerezése, rugalmas gondolkodás, problémamegoldás	
2.	Vonalkód megismerése	Problémaérzékenység, gondolkodási sebesség, egymásra figyelés, ismeretek rendszerezése, rugalmas gondolkodás, problémamegoldás	Eszközök: Vonalkóddal ellátott könyvek (páronként kettő) Tanulói munkafüzet: A vonalkódban használt háromféle kód
III. ISBN szám			
	Ráhangolódás:Az ISBN szám „megfejtése"	Elemző képesség, együttműködési képesség, problémaérzékenység	Eszközök: ISBN számmal ellátott könyvek
1.	Az ellenőrző jegy megismerése	Elemző képesség, együttműködési képesség, problémaérzékenység	
2.	Számrendszerek használata kódolásra	Elemző képesség, együttműködési képesség, problémaérzékenység	Eszközök: Csoportonként 5 db azonos fémpénz
3.	Verseny	Elemző képesség, együttműködési képesség, problémaérzékenység	

I. KRIPTOGRÁFIA

Ráhangolódás (kb. 10 perc)

Ha üzenetet szeretnénk valakinek küldeni, és nincs lehetőségünk a közvetlen átadásra (hanggal, képpel stb.), de számunkra nagyon fontos, hogy az üzenet tartalmát más ne értse meg, akkor „kénytelenek vagyunk” titkosítani, rejtjelezni, kódolni az üzenetet. Ha ez csak egy-két ember magánügye lenne, nem lenne érdemes vele foglalkozni.
Manapság az információ egyre értékesebb árucikk. Már telefonhívásaink is műholdakról verődnek vissza, e-mailjeink számos komputeren haladnak keresztül, és így mindkettő könnyűszerrel lehallgatható, elfogható, és ezzel a közölt információt „bárki” megismerheti. A szerzett információval való visszaélés komoly károkat okozhat embereknek, cégeknek, országoknak.
Az üzenetek, adatok titkosságának biztosításával a kriptográfia foglalkozik, és a rejtjelezéssel, illetve a rejtjelek megfejtésével foglalkozó embereket kriptográfusoknak nevezik. Aki többet is szeretne tudni a rejtjelezés és rejtjelfejtés történetéről, ajánlom Simon Singh: *Kódkönyv* című könyvét. Rendkívül olvasmányos, és szórakoztató mű.

1. Átrendezéses és behelyettesítéses kódolás

(Javasolt idő: 20 perc. Eszközigény: Ábécé táblázat minden párnak, csoportonként másolat Az üzenetek c. mellékletből. Munkaforma: Két pár alkot egy csoportot.)

A kriptográfiának, a rejtjelezésnek két nagy alapmódszere van: az egyik az **átrendezéses**, a másik a **behelyettesítéses kódolás**.
Az átrendezéses kódolásnál (permutációnál) a küldeni kívánt üzenet betűit (karaktereit) keverik össze valamilyen előre egyeztetett algoritmus (eljárás) szerint.
A behelyettesítéses kódolásnál a küldendő üzenet ábécéjének minden betűje egy másik betűvel (karakterrel) kerül helyettesítésre.

Válasszatok magatoknak párt! Két pár üzenetet fog váltani egymással. Mindkét pár tervezzen egy-egy kódrendszert: az egyik egy átrendezésest, a másik pár pedig egy behelyettesítésest! (Természetesen beszéljétek meg előre, ki melyik fajtát dolgozza ki.)
A dekódoláshoz (megfejtéshez) szükséges információkat mindkét pár írja le, és azt „juttassa el” a másik párhoz!

Amikor már minden pár birtokában ott van a saját és a másik pár kódrendszere is, adok mindkét párnak egy-egy üzenetet, és azt mindkét pár lekódolja a saját tervezésű kódjával. Ezek után elküldi a másik párnak a kódolt üzenet, akik azt, reméljük, megfejtik. Ezek után mindkét pár ír egy választ az üzenetre a másik pár kódrendszerével kódolva, majd visszaküldi azt!
Válasszák ki a párok a levelezőpartnereket! A munkafüzetben megtaláljátok a magyar ábécét tartalmazó táblázatot két példányban, ez meggyorsíthatja a behelyettesítéses kód tervezését. A másik példány majd használható a megfejtéshez.

Tanulói munkafüzet: Ábécé a behelyettesítéses kódrendszer kialakításához

Ha nem 4-gyel osztható a jelenlévők száma, akkor ne ahhoz a megoldáshoz folyamodjunk, hogy növeljük a csapat (a pár) létszámát, inkább a négyesekből kimaradók esetében egy-egy ember, vagy egy ember és egy pár váltson üzenetet!

Szándékosan ne adjunk több információt a két alapvető kódolási módról, így kellő teret kap a tanulók fantáziája. Érdemes a kódrendszerek értelmezésébe az algoritmus szót „becsempészni”, főleg akkor, ha eddig még nem használtuk.

Ha mindkét pár elkészítette a maga kódrendszerét, akkor már adom is az üzeneteket!

Melléklet a tanároknak: Az üzenetek

Ne dolgozzatok hangosan, mert akkor kódolás nélkül is meghallja a partner az üzenet! Most azt feltételezzük, hogy nincs mód közvetlen szóbeli közlésre, sem telefonálásra.

A párok úgy üljenek le a teremben, hogy a párpartnerek minél messzebb kerüljenek egymástól.

Ha valamelyik „négyes” már elkészült a válasz megfejtésével is, adjunk a kezükbe egy általunk kódolt rövid szöveget megfejtésre! Ne áruljuk el, hogy melyik módon kódoltuk a szöveget!

Melléklet a tanároknak: A kódolt szöveg és megoldása

Érdekességként itt megemlíthetjük az anagrammát is. Az Idegen szavak és kifejezések szótárában ezt olvashatjuk róla: az anagramma „valamely szó betűinek felcserélésével alkotott más szó”. Egy 1937-bõl származó képeslapban fedezték föl, hogy valaki négyféleképpen csoportosította Arany János nevét! Először: Anyján a sor. Majd: Jónás nyara. Harmadszor: Jó árnyasan... Végül: Anyós járna...

2. Gyakoriság, relatív gyakoriság

(Javasolt idő: 15 perc. Eszközigény: egy hosszabb szöveg bekezdései – a csoport minden tagjának más. Munkaforma: egyéni.)

Látom, sok ügyes kriptográfus van közöttetek! Persze, ha nem ismerjük a kódot, nem könnyű megfejteni (dekódolni) egy üzenetet. De mindig is éltek a világon ügyes emberek, akiknek hobbija vagy első számú feladata a rejtjelek megfejtése volt. Nos, a behelyettesítéses kód évszázadokig elég biztonságosnak tűnt, de a gyakorisági elemzés fejlődése ezt a biztonságot megszüntette.

Mi is az a gyakorisági elemzés?

Ehhez először a gyakoriság fogalmával célszerű megismerkednetek. Ha véletlenszerűen kiválasztotok egy magyar nyelven írt hosszabb szöveget, és abban összeszámoljátok, hogy melyik betű (karakter) hányszor fordul elő, és a kapott számokat leírjátok, akkor az egyes betűk gyakoriságát jegyeztétek le. Ezek a számok természetesen attól is függnek, hogy hány karakterből állt a kiválasztott szöveg. Ezért még használhatóbb táblázatunk lenne, ha kiszámolnánk, hogy az egyes betűk a teljes szöveg betűszámának hány százalékában fordul elő. Mit gondoltok, a magyar nyelvben melyik betű fordul elő a leggyakrabban?

Az e betű (hang) a leggyakoribb a magyar nyelvben.

Hajtsunk végre mi is egy kísérletet! Kifénymásoltam egy könyvből néhány oldalt, és szétvágtam a szöveget bekezdésenként. Mindenki kap egy ilyen bekezdést.

Először számoljátok meg, hogy hány betűből áll a bekezdés, jegyezzétek le! A kettős mássalhangzókat két betűnek tekintsétek! Majd mindenki számolja össze az „e”, az „a” és mondjuk a „p” betűk előfordulásának számát, azaz ezeknek a betűknek a gyakoriságát!

Összesítsük az eredményeket! Először nézzük meg, hogy a teljes szöveg hány betűből állt! Sorban mondjátok be a számokat! Kérem, hogy legalább három ember üsse is be a gépbe a hallott számokat – így egymást is ellenőrizhetitek!
Ugyanígy mondjátok be az „e” betűk, majd a többi betű gyakoriságát is!
Számoljátok ki mind a három betű relatív gyakoriságát!

Találtam egy táblázatot, amelyben 10 000 karakterből álló magyar szövegben előforduló betűk relatív gyakoriságát tüntették fel.

Íme:

Betű	**E**	**A**	**T**	**S**	**L**	**N**	**K**	**O**	**Z**	**I**	**R**	**M**	**É**
%	9,71	9,35	7,87	6,57	6,30	5,47	5,35	4,47	4,46	4,39	4,22	3,92	3,87

Betű	**Á**	**G**	**Y**	**Ö**	**V**	**B**	**D**	**U**	**H**	**J**	**P**	**Ü**	**F**
%	3,72	3,55	2,21	2,14	1,81	1,72	1,71	1,29	1,23	1,21	1,04	0,93	0,88

Betű	**C**		**X**	**W**	**Q**
%	0,60		0,01	0,00	0,00

A táblázatot – mint látható – csökkenő relatív gyakoriság szerint rendezték. Vessük össze a mi kísérletünk eredményeivel!

Mit gondoltok, miért könnyítette meg a rejtjelfejtők munkáját a betűk relatív gyakoriságának ismerete?
A kódolt szöveg elemzését már azzal kezdhették, hogy megvizsgálták, melyik karakter hányszor fordul elő a szövegben, s ez már komoly támpontot nyújthatott a további elemzéshez. Sejtést fogalmazhattak meg, hogy (egy magyar nyelven írt kódolt szövegben) a leggyakrabban előforduló karakter valószínűleg az „e” betű kódja. Természetesen egy dekódolás sikeres végrehajtásához még nagyon sokféle szempont szerint meg kell vizsgálni a szöveget, de a gyakoriságelemzés kifejlődése nagy előnyhöz juttatta a rejtjelfejtőket a rejtjelezőkkel szemben. Ekkor született meg egy sokáig feltörhetetlennek hitt kódolási mód.

Akinek felkeltettem az érdeklődését, olvashat róla a már említett Simon Singh: *Kódkönyv* című könyvének 54. oldalán.

I. MELLÉKLET A TANÁROKNAK

1. Átrendezéses és behelyettesítéses kódolás

Az üzenetek:

---

1. üzenet:

A LEGKÖZELEBBI MATEK ÓRÁN DOLGOZATOT FOGUNK ÍRNI.
NE ADJÁTOK TOVÁBB A HÍRT!
A FIZIKA DOGA IDŐPONTJÁRÓL TUDTOK VALAMIT?

---

2. üzenet:

HOLNAP GYERTEK REGGEL FÉL ÓRÁVAL ELŐBB A SULIHOZ!
UGYE TI IS A BUSZ UTOLSÓ SORÁBA AKARTOK ÜLNI?
MÁSNAK NE SZÓLJATOK ERRŐL!

A kódolt szöveg és megoldása:

E K R K E K E S E C B O M G O A I K C S Z A S T T A N D L A A C L Y U A S K

Megfejtés:
KEREKECSKE GOMBOCSKA ITT SZALAD A NYULACSKA

A kódolandó szöveget 5 karakterenként bontották szakaszokra (az utolsó szakaszban 3 betű maradt). Jelölje egy-egy szakaszban lévő 5 betűt az 1, 2, 3, 4, 5 számok ebben a sorrendben. Tekintsük mindegyik „ötösnek” a 45312 permutációját. Így megkapjuk a kódolt szöveget. Dekódoláskor az algoritmust visszafelé alkalmazzuk.

1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
K	E	R	E	K	E	C	S	K	E	G	O	M	B	O	C	S	K	A	I	T	T	S	Z	A	L	A	D	A	N

1	2	3	4	5	1	2	3
Y	U	L	A	C	S	K	A

Tanulói munkafüzet:

I. KRIPTOGRÁFIA

Az adatok továbbításának három fő problémája van: a biztonság, a titkosság és a tömörség. A biztonság kérdésével a kódelmélet, a titkosságéval a kriptográfia, a tömörséggel az információelmélet foglalkozik.
Mi két fő kérdéssel foglalkozunk: a titkossággal és a biztonsággal.

1. Átrendezéses és behelyettesítéses kódolás

Ha üzenetet szeretnénk valakinek küldeni, és nincs lehetőségünk a közvetlen átadásra (hanggal, képpel stb.), de számunkra nagyon fontos, hogy az üzenet tartalmát más ne értse meg, akkor „kénytelenek vagyunk” titkosítani, rejtjelezni, kódolni az üzenetet. Ha ez csak egy-két ember magánügye lenne, nem lenne érdemes vele foglalkozni.
Manapság az információ egyre értékesebb árucikk. Már telefonhívásaink is műholdakról verődnek vissza, e-mailjeink számos komputeren haladnak keresztül, és így mindkettő könnyűszerrel lehallgatható, elfogható, és ezzel a közölt információt „bárki” megismerheti. A szerzett információval való visszaélés komoly károkat okozhat embereknek, cégeknek, országoknak.
Az üzenetek, adatok titkosságának biztosításával a kriptográfia foglalkozik, és a rejtjelezéssel, illetve a rejtjelek megfejtésével foglalkozó embereket kriptográfusoknak nevezik. Aki többet is szeretne tudni a rejtjelezés és rejtjelfejtés történetéről, ajánlom Simon Singh: *Kódkönyv* című könyvét. Rendkívül olvasmányos, és szórakoztató mű.

Ábécé a behelyettesítéses kódrendszer kialakításához:

Karakter	Kód
A	
Á	
B	
C	
D	
E	
É	
F	
G	
H	
I	
J	
K	
L	
M	
N	
O	
P	
Q	
R	
S	
T	
U	
Ü	
V	
W	
X	
Y	
Z	

Karakter	Kód
A	
Á	
B	
C	
D	
E	
É	
F	
G	
H	
I	
J	
K	
L	
M	
N	
O	
P	
Q	
R	
S	
T	
U	
Ü	
V	
W	
X	
Y	
Z	

II. VONALKÓD

Ráhangolódás (kb. 10 perc)**:**

Mit írok most le? 010-000-011-000-1011-0-10-00

(Egy számsorozat első 8 tagját látjuk; jelsorozatot; kettes számrendszerben felírva a következő számokat: 2-0-3-0-11-0-2-0.)

És, ha ezt írom le?
– . – / – – – / – . . / – – – / . – . . / – / . – / – – /

Morzeábécével írtam le valamilyen üzenetet. Ahhoz, hogy az üzenetet meg tudjátok fejteni, szükségetek van a morzeábécére. Ettől persze ez nem titkosírás, hiszen aki ismeri a morzeábécét, könnyen elolvashatja az üzenetet. A morzeábécét elég sokáig használták üzenetek továbbítására. Két betűt biztos ismertek: az S-et és az O-t.

(S.O.S. a vészjel, állítólag a Save Our Souls! (Mentsétek meg lelkünket!) rövidítése. Van olyan vélemény, hogy a vészjel nem S.O.S., hanem S.O. Ez ismétlődik sokszor egymás után. A morzeábécében ezek válnak el egymástól a legélesebben, és legjobban megkülönböztethetők a többi betűtől: ...---, tititi-tátátá és így tovább a végtelenségig.)

A munkafüzetben megtaláljátok a morzeábécét.

Tanulói munkafüzet: Morzeábécé

Mint látható, a nemzetközi morzeábécében nincs kódja a hosszú magánhangzóknak. Ez nem gátolja persze a megfejtést. (*KÓDOLTAM*) Új értelmezést adhatunk az először felírt szám-, vagy jelsorozatnak is. Figyeljétek meg, itt is két jelet használtam: a 0-t és az 1-et!

Ez azonosítható a morzeábécé kódjával: vonal helyett a 0, a pont helyett az 1.

1. A morzeábécé

(Javasolt idő: 10 perc. Eszközigény: morzeábécé. Munkaforma: párban.)

Mit tudtok a morzeábécé keletkezéséről? Kiről nevezték el?

1839-ben Angliában Sir Charles Wheatstone és William Fothergill Cooke mágneses tűkből épített detektorokat, amelyek a beérkező elektromos jel hatására kitértek. Néhány évvel később Samuel Morse Amerikában Baltimore-t és Washingtont (60 km távolság) kötötte össze telegráffal (távíróval), és egy elektromágnessel felerősítette a jelet, miáltal a célállomáson még elég erős volt ahhoz, hogy rövid és hosszú jeleket – pontokat és vonalakat – rajzoljon egy papírra. Az ő nevéhez fűződik a ma már közismert morzeábécé kidolgozása is.)

Alakítsatok ki párokat, és írjatok egymásnak egy rövid levelet morzeábécével! Ezután „küldjétek el” egymásnak a levelet, és olvassátok is el!

2. Vonalkód

(Javasolt idő: 25 perc. Eszközigény: Vonalkóddal ellátott könyvek (páronként kettő). Munkaforma: frontális, majd párban.)

Ha megoldható, érdemes ezt a foglalkozást az iskola könyvtárában tartani, így több könyv kódját is megvizsgálhatják a tanulók.

Foglalkozzunk egy keveset a kódolás biztonságának kérdésével is!

A kódolások során legtöbb esetben egy üzenetből számsorozatot készítenek. Nagyon gyakran előfordul, hogy a kódolt üzenetek számsorozatát a 0 és 1 számjegyekből alkotjuk, hiszen ezt elektromos berendezéssel könnyű megvalósítani (folyik az áram – nem folyik az áram). Az üzenet hossza gyakran rögzített.

Kódokkal a mindennapi életben is gyakran találkozunk. Ha bemegyünk egy bevásárlóközpontba, a megvásárolt árucikket a pénztárnál vonalkód segítségével azonosítják.

Vegyétek kézbe a kikészített könyveket!
Vizsgáljátok meg a könyvek vonalkódját! Mit láttok?

A vonalkód felett egy ISBN számot, alatta különböző vastagságú sötét és fehér vonalakat, és ez alatt egy 13 számjegyből álló számot láthatunk. A vonalkód ebből a 13 jegyből álló számból készül. Ez a 13 számjegy az „üzenet”. A 13 számjegy mindegyikét 0-ból és 1-esből álló 7-tagú számsorozattal kódolják. Egy-egy számjegy kódja háromféle lehet: A vagy B vagy C típusú. Íme a háromféle kód:

Melléklet tanulóknak: A vonalkódban használt háromféle kód

Az „A” jelkészlettel	A „B” jelkészlettel	A „C” jelkészlettel
0 : 0001101	0 : 0100111	0 : 1110010
1-es: 0011001	1-es: 0110011	1-es: 1100110
2-es: 0010011	2-es: 0011011	2-es: 1101100
3-as: 0111101	3-as: 0100001	3-as: 1000010
4-es: 0100011	4-es: 0011101	4-es: 1011100
5-ös: 0110001	5-ös: 0111001	5-ös: 1001110
6-os: 0101111	6-os: 0000101	6-os: 1010000
7-es: 0111011	7-es: 0010001	7-es: 1000100
8-as: 0110111	8-as: 0001001	8-as: 1001000
9-es: 0001011	9-es: 0010111	9-es: 1110100

A vonalkódban a 0-kat fehér, az 1-eseket sötét vonal jelöli. Eszerint két egymás utáni 1-est dupla vastagságú sötét vonal, három 0-t három egység szélességű fehér vonal jelöl. Ezen kívül vannak a széljelek (a kódjuk: 101, tehát sötét – fehér – sötét vonalak jelzik), és középen az elválasztójel (kódja: 01010, tehát fehér – sötét – fehér – sötét – fehér vonalak jelzik).
A vonalkód egy leolvasó készülékkel olvasható el: A fekete és a fehér csíkok eltérő mértékben verik vissza a fényt, amit a leolvasó készülék érzékel és értelmez (dekódol), majd az adatokat továbbítja a számítógépnek.
Ez a fajta vonalkód 13 számjegyből áll. Ezt úgy nevezik, hogy EAN-13 rendszerű vonalkód (European Article Numbering System). Nézzétek csak meg, hogy a könyvetek vonalkódján milyen szám áll balról számolva az első három helyen?

978. Ez a három számjegy arra utal, hogy ez egy könyv vonalkódja. Minden, ezt a rendszert használó gyártónak van ún. országkódja, ami jelzi, hogy melyik országban gyártott termékről van szó, és ez a három szám a kód első három számjegye. Magyarországé 599.
Ha könyv a termék, akkor 978 az első három számjegy.
Az első három számot követő számok „üzenete” a következő: 4–7.-ig a terméket gyártó vállalat azonosítója, 8–12. pedig a termék azonosítója, a 13. szám ún. ellenőrző szám (erről később még lesz szó).
Vegyétek alaposabban szemügyre a könyv vonalkódját! A középső elválasztójeltől balra illetve jobbra lévő 6-6 számról próbáljátok kideríteni, hogy melyik szám melyik jelkészlettel lett kódolva!
Az első szám a 7-es. Nézzétek meg figyelmesen, hogy a három jelkészlet milyen kódot ad a 7-esnek, majd vegyétek szemügyre a sötét és fehér vonalakat! A-val, B-vel vagy C-vel lett kódolva?

(A-val. A bal oldali 6 szám A-val vagy B-vel valamilyen sorrendben, a jobb oldali 6 szám pedig mind C jelkészlettel kódolt.)

Ha sikerült megfejteni minden számjegy kódját, cseréljétek ki a könyveket, és ellenőrizzétek egymás megfejtését!

Térjünk vissza a 13. számra, az ellenőrző számra! Gyakran előfordul, hogy a vonalkód-leolvasó sikertelenül próbálkozik, ilyenkor a pénztáros megismétli az eljárást, majd sikertelenség esetén manuálisan beüti 13 számot. Ha valamelyik számjegyet tévesen írja be, a műszer jelzi, hogy nem sikerült a beolvasás. Ugyanez történik akkor is, ha megsérül a vonalkód, vagy gyűrődés miatt nem leolvasható le, a gép jelzi, és nem egy másik termék – esetleg drágább – kódját olvassa le. Tehát a hiba felismerésének lehetősége be van építve a kódba. Erre szolgál a 13. szám.
Az ellenőrző 13. szám az első 12-ből alapműveletekkel előállítható:

Adjátok össze a páratlan helyeken lévő számokat! (A 13.-at ne adjátok hozzá!) Jelöljük ezt az összeget D-vel. Ezután a páros helyeken lévő számokat is adjátok össze (jelöljük az összeget E-vel.). Ha az E-t megszorozzuk egy bizonyos számmal, és a kapott számhoz hozzáadjuk D-t, és ezt az összeget kipótoljuk egy olyan egyjegyű számmal, hogy 10-zel osztható számhoz jussunk, akkor ez a „pótló szám” a keresett 13. szám.

Például: Legyen a vonalkód: 9 7 8 9 6 3 8 6 7 6 2 2 **1.**
A páratlan helyeken lévő számok összege: $D = 40$.
A páros helyeken lévő számok összege: $E = 33$.

Ha a 33-at megszorozzuk egy pozitív egész számmal (jelöljük ezt n-nel), akkor $33n + 40 + 1$ egy tízzel osztható szám. Melyik szám lehet az n?

(Csak a 3 lehet, hiszen a 33-nak – az egyjegyűek közül – csak a 3-szorosa végződik 9-re.)

Vizsgáljátok meg, hogy a nálatok lévő könyvek esetében is így számítódott-e ki az utolsó szám!
Nézzük meg, hogy a kódba beillesztett ellenőrző szám milyen hiba kiküszöbölését teszi lehetővé! Észre veszi-e a gép, ha a pénztáros egy számjegy helyett egy másikat üt be?

(Ezt a hibát kiszűri az ellenőrző szám.)

És ha két szomszédos számot felcserél?

(Nem feltétlenül. Ha a felcserélt két szomszédos szám különbsége 5 (például a példánkban szereplő vonalkódban a 3-as és 8-as felcserélése), akkor ugyanaz az ellenőrző szám, tehát az ellenőrző szám ezt a hibát nem szűri ki.)

Azt vajon észreveszi-e a leolvasó az ellenőrző szám segítségével, ha két számjegy helyett ír be másikat?

(Nem feltétlenül. Ha a példában szereplő vonalkódban két 8-as helyett mindkét helyen 3-ast üt be a pénztáros, a végösszeg tízes maradéka nem változik, tehát az ellenőrző szám ugyanaz marad.)

A következő foglalkozásra egy kis kutatómunkát ajánlok. A könyvek vonalkódja felett minden esetben látható egy ún. ISBN (International Standard Book Number) szám. Nézzetek meg minél több ilyen számot, gyűjtsetek össze belőle minél többet! Próbáljátok kitalálni, hogy hogyan épül fel ez az azonosító! Segítségül annyi, hogy ebben is az utolsó számjegy egy ellenőrző jegy, amelynek értéke meghatározható a többi jegyből, és ezzel nemcsak egy számjegy elírásából adódó hibát lehet kiszűrni, hanem két tetszőleges jegy felcserélésével adódót is.

Tanulói munkafüzet
II. VONALKÓD

1. A morzeábécé

Morzeábécével írtam le valamilyen üzenetet:
– . – / – – – / – . . / – – – / . – . . / – / . – / – – /

Ahhoz, hogy az üzenetet meg tudjátok fejteni, szükségetek van a morzeábécére. Ez persze nem titkosírás, hiszen aki ismeri a morzeábécét, könnyen elolvashatja az üzenetet. A morzeábécét elég sokáig használták üzenetek továbbítására. Két betűt biztos ismertek: az S-et és az O-t.

(S.O.S. a vészjel, állítólag a Save Our Souls! (Mentsétek meg lelkünket!) rövidítése. Van olyan vélemény, hogy a vészjel nem S.O.S., hanem S.O. Ez ismétlődik sokszor egymás után. A morzeábécében ezek válnak el egymástól a legélesebben, és legjobban megkülönböztethetők a többi betűtől: ...---, tititi-tátátá és így tovább a végtelenségig.)

A nemzetközi morzeábécé:

Karakter	Kód	Karakter	Kód	Karakter	Kód
A	.–	P	.––.	5	.....
B	–...	Q	––.–	6	–....
C	–.–.	R	.–.	7	––...
D	–..	S	...	8	–––..
E	.	T	–	9	––––.
F	..–.	U	..–	0	–––––
G	––.	V	...–	pont	.–.–.–
H	....	W	.––	vessző	––..––
I	..	X	–..–	kérdőjel	..––..
J	.–––	Y	–.––	kettőspont	–––...
K	–.–	Z	––..	pontosvessző	–.–.–.
L	.–..	1	.––––	kötőjel	–...–
M	––	2	..–––	ferde törtvonal	–..–.
N	–.	3	...––	idézőjel	.–..–.
O	–––	4	....–		

2. Vonalkód

Foglalkozzunk egy keveset a kódolás biztonságának kérdésével is!
A kódolások során legtöbb esetben egy üzenetből számsorozatot készítenek. Nagyon gyakran előfordul, hogy a kódolt üzenetek számsorozatát a 0 és 1 számjegyekből alkotjuk, hiszen ezt elektromos berendezéssel könnyű megvalósítani (folyik az áram – nem folyik az áram). Az üzenet hossza gyakran rögzített.
Kódokkal a mindennapi életben is gyakran találkozunk. Ha bemegyünk egy bevásárló központba, a megvásárolt árucikket a pénztárnál vonalkód segítségével azonosítják.
Vegyétek kézbe a kikészített könyveket!
Vizsgáljátok meg a könyvek vonalkódját! Mit láttok?
A vonalkód felett egy ISBN számot, alatta különböző vastagságú sötét és fehér vonalakat, és ez alatt egy 13 számjegyből álló számot láthatunk. A vonalkód ebből a 13 jegyből álló számból készül. Ez a 13 számjegy az „üzenet". A 13 számjegy mindegyikét 0-ból és 1-esből álló 7-tagú számsorozattal kódolják. Egy-egy számjegy kódja háromféle lehet: A vagy B vagy C típusú.

A vonalkódban használt háromféle kód:

Az „A" jelkészlettel	A „B" jelkészlettel	A „C" jelkészlettel
0 : 0001101	**0 : 0100111**	**0 : 1110010**
1-es: 0011001	**1-es: 0110011**	**1-es: 1100110**
2-es: 0010011	**2-es: 0011011**	**2-es: 1101100**
3-as: 0111101	**3-as: 0100001**	**3-as: 1000010**
4-es: 0100011	**4-es: 0011101**	**4-es: 1011100**
5-ös: 0110001	**5-ös: 0111001**	**5-ös: 1001110**
6-os: 0101111	**6-os: 0000101**	**6-os: 1010000**
7-es: 0111011	**7-es: 0010001**	**7-es: 1000100**
8-as: 0110111	**8-as: 0001001**	**8-as: 1001000**
9-es: 0001011	**9-es: 0010111**	**9-es: 1110100**

A vonalkódban a 0-kat fehér, az 1-eseket sötét vonal jelöli. Eszerint két egymás utáni 1-est dupla vastagságú sötét vonal, három 0-t három egység szélességű fehér vonal jelöl. Ezen kívül vannak a széljelek (a kódjuk: 101, tehát sötét – fehér – sötét vonalak jelzik), és középen az elválasztójel (kódja: 01010, tehát fehér – sötét – fehér – sötét – fehér vonalak jelzik).
A vonalkód egy leolvasó készülékkel olvasható el: A fekete és a fehér csíkok eltérő mértékben verik vissza a fényt, amit a leolvasó készülék érzékel és értelmez (dekódol), majd az adatokat továbbítja a számítógépnek.
Ez a fajta vonalkód 13 számjegyből áll. Ezt úgy nevezik, hogy EAN-13 rendszerű vonalkód (European Article Numbering System). Nézzétek csak meg, hogy a könyvetek vonalkódján milyen szám áll balról számolva az első három helyen?
978. Ez a három számjegy arra utal, hogy ez egy könyv vonalkódja. Minden, ezt a rendszert használó gyártónak van ún. országkódja, ami jelzi, hogy melyik országban gyártott termékről van szó, és ez a három szám a kód első három számjegye. Magyarországé 599.
Ha könyv a termék, akkor 978 az első három számjegy.
Az első három számot követő számok „üzenete" a következő: 4–7.-ig a terméket gyártó vállalat azonosítója, 8–12. pedig a termék azonosítója, a 13. szám ún. ellenőrző szám (erről később még lesz szó).
Vegyétek alaposabban szemügyre a könyv vonalkódját! A középső elválasztójeltől balra illetve jobbra lévő 6-6 számról próbáljátok kideríteni, hogy melyik szám melyik jelkészlettel lett kódolva!
Az első szám a 7-es. Nézzétek meg figyelmesen, hogy a három jelkészlet milyen kódot ad a 7-esnek, majd vegyétek szemügyre a sötét és fehér vonalakat! A-val, B-vel vagy C-vel lett kódolva?

III. ISBN SZÁM

Ráhangolódás (kb. 10 perc)

Minden magyar könyv ISBN száma 10 jegyű, és 963-mal kezdődik. Az utána következő – elválasztó jelek közötti – szám a kiadót azonosítja, majd az ezt követő a könyvet, s végül az utolsó az ellenőrző számjegy.
Sikerült valakinek rájönni, hogy milyen módon állítható elő ez az utolsó számjegy az előtte álló 9 számjegyből?

Azt akarjuk, hogy számjegycserekor más szám jöjjön ki a végére. Azt már láttuk, hogy ha minden másodikat ugyanazzal a számmal szorozzuk, akkor ezzel nem feltétlen szűrhető ki a cseréből adódó hiba. Próbálkozzunk úgy, hogy minden számjegyet más számmal szorozzunk meg! 9 szám van. Mi legyen a 9 különböző szám, amikkel sorban megszorozzuk az ISBN számjegyeket?
Próbáljuk ki: az első számjegyet 9-cel, a következőt 8-cal, és így tovább, a 9-ediket 1-gyel szorozzuk, majd adjuk össze a szorzatokat, s a vonalkód mintájára pótoljuk a kapott számot a legközelebbi 10-zel osztható számra. A pótló szám az utolsó számjegy lett?

Nem. Mást kellene kitalálnunk.
Nem tudom, láttatok-e olyan ISBN számot, amelyben az ellenőrző számjegy helyén X áll? Az ellenőrző számjegy 0, 1, 2, …, 8, 9, X lehet. Az X valószínűleg a kétjegyű 10-es számot helyettesíti. Tehát 11-féle lehet a pótló szám. Ezek szerint nem 10-zel osztható számra pótolja ki az ellenőrző szám az első számjegyekből kapott összeget, hanem 11-gyel oszthatóra. Nézzük meg az előbb kapott összegnél, hogy az ellenőrző jegyet kapjuk-e, ha a legközelebbi 11-gyel oszthatóra pótoljuk ki az összeget!
Még mindig nem jó. Mit tudunk még változtatni? Mi lenne, ha nem 9-cel, hanem 10-zel kezdenénk a számjegyek szorzását?
Győzelem!

1. Az ellenőrző jegy

(Javasolt idő: 10 perc. Eszközigény: Könyvek vagy azok hátlapjának fénymásolatai. Munkaforma: egyéni.)

Jó lenne legalább egy ISBN számnál ellenőrizni, hogy bármelyik két számjegyének felcserélésével létrejövő hibát az ellenőrzőjegy kiszűri-e! Nézzük a következő ISBN kódszámot:
963-9132-57-8

Hány cserét lehet végrehajtani?

Módszeresen számoltassuk össze: 9-6, 9-3, 9-1, 9-3, …, 7-8

Éppen 17-en vagytok, így a 34 cserével létrehozott számoknak az ellenőrző jegyét gyorsan meg tudjuk nézni. Mindenki vállaljon el kettőt! Osszátok szét a „cseréket”! Kapott valaki 8-as ellenőrző jegyet?
Ha valaki kedvet kapott hozzá, próbálja bebizonyítani, hogy egy $x_1x_2x_3...x_9n$ ISBN számban, ahol n jelöli az ellenőrző jegyet, bármelyik két számjegyet felcseréli, a kapott új szám ellenőrző jegye nem lehet n.

2. Számrendszerek használata kódolásra

(Javasolt idő: 15 perc. Eszközigény: csoportonként 5 db azonos pénzérme. Munkaforma: csoportban.)

Alakítsatok ki 3 fős csoportokat! Minden csoport kap 5 egyforma pénzérmét. Találjatok ki olyan kódrendszert (a számrendszerek felhasználásával), amellyel 0-tól valamilyen (a csoport által kitalált) n pozitív számig minden számot le tudtok kódolni ezekkel a pénzérmékkel az üres tanári asztalon! Ha egy csoport kitalált egy ilyen kódrendszert, jelezze, hogy meddig tud kódolni (mennyi az n)!

Amelyik csoport a legnagyobb számot mondja be, az lehetőséget kap kódrendszerük bemutatására: a csoport egyik tagja kimegy, én mondok egy számot (amelyik természetesen az általuk megjelölt legnagyobb számnál nem nagyobb), és a csoport bennmaradt tagjai lekódolják a tanári asztalon a számot. Ekkor behívjuk a társukat, aki kitalálja a számot. Ha nem sikerül, akkor a következő (az előbbinél kisebb számot bemondó) csoport kap lehetőséget a kódrendszerük bemutatására.

Ha a „fej” jelenti például a 0-t, és az „írás” az 1-esnek felel meg, akkor kettes számrendszert használva 31-ig minden szám kódolható az 5 pénzérmével. Ha kihasználják azt is, hogy a pénzérmén a fej vagy írás hogyan áll (4-féle irányban állhat), akkor 5-ös számrendszerig is elmehetnek, és ekkor 3124-ig minden pozitív egész számot tudnak kódolni. (Természetesen ekkor meg kell egyezniük, hogy melyik állás melyik számjegyet jelöli.)

Hibalehetőség: nem beszélik meg előre a gyerekek, hogy honnan olvassák a kódolt számot.

3. Verseny

(Javasolt idő: 10 perc. Eszközigény: feladatlap. Munkaforma: csoportban.)

A táblára felírok egy 10 jegyből álló, 0 és 1 jelek felhasználásával létrehozott kódolt adatot. A végére írok egy ellenőrző jegyet. Ennek az a szerepe, hogy ha a 10 jel valamelyike megváltozik, akkor ez jelzi, hogy hiba történt.

Összesen négy ilyen kódolt adatot írok fel (11 jellel), de a negyediknél az utolsó jegyet (az ellenőrző jegyet) nem írom le. Ha valamelyik csoport tudja, hogy mi lesz az utolsó jegy, kézfeltartással jelezze! Ha helyesen adja meg az utolsó jegyet, akkor a csoport megszerzi a jogot a folytatásra: én csak az első 10 jelet írom fel, és ők mondják meg az utolsót. Ha elrontják, a folytatást egy másik csoport veheti át.

Nos, az első három:
1001100101 **1**
1110001000 **0**
0011111011 **1**
0111010110 **?**

(Az utolsó jegy annak megfelelő, hogy a 11 jegyben az 1-esek száma páros vagy páratlan. Ha az első 10 jegy közül pontosan egy megváltozik, ezzel megváltozik az 1-esek számának paritása, és az utolsó jegy jelzi a hibát.)

Az elsőként elkészült csoport mutassa be a megoldást!

A többiekhez szól a kérdés:

Ha valamilyen oknál fogva a 10 jegyű kódban pontosan egy jegy megváltozik, akkor miért tudja az ellenőrző jegy a hibát jelezni?

Ha marad rá idő, a versenyt a következő probléma kitűzésével folytassuk.

Egy hajó és utasai, összesen 100 fő, Ungabunga szigetén az emberevők fogságába esett. Tudják, hogy másnap reggel a kannibálok leültetik őket egymás mögé, és mindegyikük fejére egy-egy piros vagy kék sapkát húznak. Mindenki csak az összes előtte ülő ember fején lévő sapkát fogja látni, a sajátját és a mögötte ülőkét nem. A leghátsó embertől kezdve sorban mindenki hangosan mondhat majd egy színt: pirosat vagy kéket. A végén azt engedik szabadon, aki saját sapkája színét mondta, aki nem találta el, azt bizony megeszik. A kannibálok szigorúak, ha bárki mást tesz, minthogy a lehető legegyszerűbben kimondja a „piros” vagy a „kék” szót, akkor senkinek sem kegyelmeznek.

A foglyoknak még egy esélye van. Most este még összebeszélhetnek. Szeretnék, hogy minél többen megszabaduljanak. Hány fogoly menekülhet meg biztosan?

Ha könnyíteni szeretnénk, a problémát tűzzük ki úgy, hogy tudjuk, hogy összesen 12 kék sapka van.

Az előkészítő feladat után talán könnyebben rájönnek a tanulók, hogy 99 rab biztosan megszabadítható. Az előző problémamegoldás módszerét alkalmazva az utolsó ember megnézi, hogy az összes előtte ülő fején pl. a kék sapkák száma milyen paritású. Előzőleg megegyeznek abban, hogy az utolsó ember – ha a kék sapkák száma páros, akkor pirosat, ellenkező esetben kéket mond. Így az őt megelőző rab, mivel látja, hogy az előtte ülők között összesen hány kék sapkás van (páros vagy páratlan számú), ha páros számú, akkor az ő fején biztosan piros, ha páratlan az előtte lévő kékek száma, akkor az ő fején kék sapka van. És így tovább, mindegyik a háta mögött ülő rab válaszából ki tudja deríteni a fején lévő sapka színét, tehát mindenki megmenekül. Az elsőnek megszólaló (leghátul ülő) rab esélye a szabadulásra 50%.

E témakörben további feladatokat találhatunk Hraskó András és Szőnyi Tamás szakköri anyagában (*Hibajavító kódok*). Elérhető a www.fazekas.hu/matek* portálon, vagy nyomtatásban: *Közös nevezőnk a matematika* című Kőszeg 2002 kiadványban, vagy az *Új matematikai mozaik*ban (Typotex, 2002).

* 2007. augusztusában elérhető a honlap.