A számok titkos élete

Információk kódolásáról, titkosításáról és kódfejtésről szóló tervezet egy középiskolai szakkörre

Szakdolgozat

Készítette:
Mécs Anna
Tanári MA
Matematika–magyar szak

Témavezető:
Dr. Freud Róbert
egyetemi docens
Algebra és Számelmélet Tanszék

Eötvös Loránd Tudományegyetem Természettudományi Kar

Budapest, 2012

Tartalomjegyzék

1. Bevezetés **4**
- 1.1. Gyújtózsinór . . . 4
- 1.2. Az utazás . . . 4
- 1.3. Mese habbal . . . 5
- 1.4. A célközönség . . . 6
- 1.5. Köszönetnyilvánítás . . . 6

2. A kerettanterv és a szakdolgozat kapcsolata **8**
- 2.1. Célok és feladatok . . . 8
- 2.2. Fejlesztési követelmények . . . 9
- 2.3. A tematikus egységek részletezése . . . 9
  - 2.3.1. Gondolkodási módszerek . . . 10
  - 2.3.2. Számtan, algebra . . . 10
  - 2.3.3. Függvények . . . 10

3. Hol van a kincs? **11**
- 3.1. Melyik országban van a kincs? . . . 11
  - 3.1.1. Gondoltam egy számra az 1 és a 2 közül. Hány kérdéssel tudod kitalálni? . . . 11
  - 3.1.2. Gondoltam egy számra az 1, 2 és 3 közül. Hány kérdéssel tudod kitalálni? . . . 11
  - 3.1.3. Gondoltam egy számra 1 és 4 között. Minimum hány kérdéssel tudod biztosan kitalálni? . . . 12
  - 3.1.4. Mi a helyzet 5, 6, 7, 8, 9 stb. szám esetén? . . . 12
  - 3.1.5. Gondoltam egy számot 1 és 4 között. Legkevesebb hány darab előre leírt kérdéssel tudhatjuk meg a választ? . . . 14
  - 3.1.6. Gondoltam egy számot 1 és 2^n között. Legkevesebb hány darab előre leírt kérdéssel tudhatjuk meg a választ? . . . 14
- 3.2. Melyik megyében van a kincs? . . . 16
  - 3.2.1. Mi a megoldás, ha nem vész el egy válasz sem? . . . 17
  - 3.2.2. Mi a megoldás, ha csak 8 dologból kell kitalálni, és úgy vész el egy válasz? . . . 17
- 3.3. A bomba hatástalanítása . . . 18
  - 3.3.1. Van 9 darab bombánk, 8 közülük azonos tömegű, viszont egy darab kicsit nehezebb. Milyen méréseket végezzünk egy kétkarú mérlegen? (Nem szükséges előre leírtakat csinálni.) . . . 18
  - 3.3.2. Van 9 darab bombánk, 8 közülük azonos tömegű, viszont egy darab kicsit nehezebb. Milyen méréseket végezzünk egy kétkarú mérlegen, ha előre le kell írni a méréseket? (Azaz, hogy melyik bomba mikor hol van a mérés alatt.) . . . 19
- 3.4. Mik a kincs pontos koordinátái? . . . 21
  - 3.4.1. Mi a helyzet, ha a 0, 1, 2,..., 9 számjegyeket mind használhatom? 21
  - 3.4.2. Mi a helyzet, ha csak a 0 és az 1 számjegyeket használhatom? 21

4. A rejtelmes város **23**
4.1. A príma kapukód . . . 23
4.2. A kőbe vésett egyenlet . . . 24
4.3. Ne légy racionális! . . . 26
4.4. A szórakozott öregurak . . . 27
4.5. A prímallergia . . . 28

5. A titkos kulcs a győzelemhez **30**
5.1. A titkos táblázat . . . 30
5.1.1. Vajon milyen összefüggés lehet a két táblázat között? . . . 31
5.1.2. Milyen megfeleltetést tudtok elképzelni? . . . 31
5.1.3. Ennek fényében mit rejthet az üzenet? . . . 31
5.1.4. Mik lehetnek az ilyen titkosítás előnyei? . . . 31
5.1.5. Mik lehetnek az ilyen titkosítás korlátai? . . . 31
5.2. Üzenj minden rubrikával! . . . 31
5.2.1. Vegyük egy kicsit szemügyre az első táblázatot! Hogy helyezkednek el benne a számok? . . . 32
5.2.2. De ezt még nem tudjuk értelmezni. Mi célt szolgálhat a többi szám? . . . 32
5.2.3. De mi lehet ennek a módszernek az egyik veszélye? . . . 32
5.3. Jani Javaslata . . . 33
5.3.1. Azt gondoljuk végig, hogy az üzenet küldője, vagy fogadója kerül nehéz helyzetbe? . . . 33
5.4. A titkos x . . . 34
5.4.1. Mit jelenthet az $x + 2$ titkos üzenet? . . . 34
5.4.2. Egy dolog még tisztázásra vár: ez a mi ,,dekódolós" szabályunk, vagy a saját szabályukat küldték el? . . . 34
5.5. Kincstári számvetés . . . 35
5.5.1. Hogyan álljunk neki? . . . 36
5.5.2. Hogyan tudjuk meg az összeget? . . . 36
5.6. Kulcskérdés . . . 37
5.6.1. Számoljuk le! . . . 37
5.7. A Nagy Háromezerkarú Osztófosztó . . . 38
5.7.1. Mi is a feladat? . . . 38
5.7.2. De hogyan okoskodjanak egy nagyobb számnál? . . . 38
5.7.3. És a prímtényezők? . . . 39
5.7.4. De mi a helyzet ha három különböző prímtényező szerepel? . . . 40
5.7.5. ,,De jó lenne általánosítani!" . . . 40
5.7.6. Hogyan alakítsuk át? . . . 41
5.8. A titkos kitevő . . . 44
5.8.1. Hogy szól a matematika nyelvén a feladat? . . . 44
5.8.2. Hogyan tudnánk a sejtés alapján bizonyítást kreálni? . . . 45
5.9. Lakat a számon . . . 47
5.9.1. Hogyan álljunk neki a lehetetlennek tűnő feladatnak? . . . 48
5.9.2. Mi a helyzet, ha a lakatokat nem fizikai értelemben képzeljük el, hanem úgy mint kódolási szabályokat? . . . 48

5.10. A kíváncsi matekos futár 48
5.10.1. Segíthet, ha leegyszerűsítjük a kérdést és matematikai köntösbe bújtatjuk! 48
5.10.2. Ez minden invertálható f és g esetén így van? Próbáljuk ki! . 49
5.10.3. Milyen elsőfokú függvénypárok lesznek alkalmasak? Gondoljuk végig általánosan! 49
5.10.4. Próbáljuk ki! 50
5.10.5. Egy kérdés még maradt: legfeljebb mennyit tudhat a minden hájjal megkent futár, hogy a titkot biztosan ne tudja kitalálni? 50
5.11. A hihetetlen titkosító eljárás 51
5.11.1. "Először egy feladványt kaptok: ha el akarjuk dönteni 1291-ről, hogy prím-e, akkor meddig kell ellenőrizni az oszthatóságot?" — Kérdezte kacsintva Izabella. 52
5.11.2. Mert kell egy N, hol egy prímszám sem látható! 53
5.11.3. Hogyan fogjuk be- és kicsomagolni az üzenetet? 54
5.11.4. Milyen kitevőre emeljük, hogy ugyanaz legyen a maradék? . . 54
5.11.5. Mindig megoldható az egyenlet? 56
5.11.6. Mit üzen nekünk RSA? 57

6. Irodalomjegyzék **58**

7. Mellékletek **60**
7.1. 1. számú melléklet: Témavezetői bírálat 60
7.2. 2. számú melléklet: A szakdolgozati konzultáció igazolólapja 61
7.3. 3. számú melléklet: Eredetiságnyilatkozat 62

1. Bevezetés

1.1. Gyújtózsinór

Amikor nekiálltam a szakdolgozatomnak, akkor ebben az ,,egyenletben" gondolkodtam:

♣ érdekes feladatok + a középiskolai matematikára épülő, azt támogató és azon túlmutató anyagrész + kultúrtörténeti vonatkozások, kapcsolat a való élettel ≈ szakdolgozat ♣

Sokat tanakodtam azon, hogy mi lehet az igényeimnek megfelelő téma. Hiszen rengeteg olyan matematikai alkalmazás van, amely nagyon izgalmas, de a matematikai hátterének megértése messzemenően meghaladja a középiskolai kereteket. Rengeteg olyan anyagrész van, amelyből szép feladatokat lehet találni, alkotni, de az alkalmazása (még) nem látható tisztán.

Hosszas gondolkodás után eszembe jutottak Juhász Péter (az ELTE TTK Számítógéptudományi Tanszék oktatója) matematikai tehetséggondozással kapcsolatos kurzusai. Az itt látott, egyszerű barkochbázásból, vagy kétkarú mérlegekkel való játékból induló feladatok végül számrendszerekhez, kódoláshoz vezettek. Nagy élményem és a szakdolgozat megírásakor meghatározó motivációm éppen ezen feladatokhoz kapcsolódik. Egyik este egy mérleges feladványon törtem a fejem a szobámban, amikor történelem szakos öcsém bejött hozzám, és nagyon érdekelte, hogy min gondolkodom. Megmutattam neki a feladatot, ő leírta, majd elrohant. Reggel arra ébredtem, hogy az asztalomon a hibátlan megoldás várt.

Ekkor még nem láttam, hogy miként lesz ebből egy egész szakdolgozat, úgyhogy tovább gondolkodtam. Témavezetőm, Freud Róbert algebrával és számelmélettel foglalkozó órái jutottak eszembe. Egyrészt a prímszámok különös világa, az oszthatósággal foglalkozó izgalmas feladatok és a sokszor emlegetett RSA-algoritmus [ez egy betűszó, kitalálói, Rivest, Shamir és Adleman neveinek kezdőbetűiből áll össze (Freud – Gyarmati 2006: 214–217)]. Gyorsan felidéztem a nyílt kulcsú titkosító eljárásról szóló részeket, és habár tudtam, hogy ez jelentősen meghaladja a középiskolában tanultakat, láttam, hogy megérthető, bizonyos elemeiben felfedezhető.

Kezdett összeállni a kép. Van egy feladatcsokor, amely a kódolás esszenciájának megmutatására kiválóan alkalmas, és saját tapasztalataim szerint is lázban tartja az embert. Van egy eljárás, amely az emberi elme nagyságára és a gépek korlátoltságára épül: nyílt kulccsal titkosítunk, mégis csak a kulcs kitalálója tudja megfejteni, méghozzá azért, mert a komputereknek még szinte lehetetlen feladat hatalmas számokat prímtényezőkre bontani. Hogyan kapcsoljam össze? Milyen lépéseken keresztül juthatok el oda, hogy e bonyolult eljárás befogadható legyen?

1.2. Az utazás

A fent vázolt témák már nagyjából kirajzoltak egy ívet. A kapcsolat, amire felfűzhetem a szakdolgozatom: egy információt kódolunk, majd azt nyílt kulcsú titkosítással

rejtjük el. Ez már lényegében sugallta a kiinduló- és a végpontot, vagy témához illően: az alfát és az ómegát.

Így szakdolgozatom első része a kódolással kapcsolatos feladatok. Ezeknél a már említett Juhász Péter-féle órák jelentették az alapot, az ott hallott feladatokhoz építettem létrát: az egészen kis kérdésektől (például 2-3 dologból hány eldöntendő kérdéssel tudjuk kiválasztani a gondolt tárgyat) egészen a matematikai általánosításig eljutunk. Törekedtem arra, hogy a főfeladatokban mindig legyen valamilyen rejtély: azaz nem árulom el, hogy mi a minimális kérdés- vagy mérésszám, hanem arra is a diákoknak kell rájönniük.

A feladatok második egységében a titkosító eljárásra rávezetésképpen a prímszámokkal foglalkozunk. Ennek célja egyfelől a tiszta matematikai feladatok szerepeltetése, az oszthatósággal való bánásmód, a ,,prímszelídítés", hiszen ezen kitüntetett számok nagy jelentőséggel bírnak a későbbiekben bemutatott algoritmusban.

A szakdolgozat utolsó és egyben legnagyobb része már kizárólag a titkosításról szól. Itt két mozgatórugót említenék: egyrészt a titkosítás megízlelése, függvényként való értelmezése, másrészt a konkrét RSA-algoritmus megértése. Ez utóbbi többek között az Euler-Fermat-tételre és az Euler-féle φ függvényre vonatkozó tételre épül. E két jelentős matematikai eredmény egyetemi szintű. Így komoly feladat volt számomra, hogy elemi lépésekre lebontva érthetővé tegyem. Igyekeztem minden kis részletét kibontani, legtöbb esetben valóban a legapróbb egységét is bizonyítjuk a szakdolgozatban. Számomra is rendkívül tanulságos volt ez a ,,cincálás", ugyanis éppen a matematikatanítás nehézségeire és szépségeire világított rá. Mivel már régóta foglalkozom matematikával, így elképzelhető, hogy tapasztalatból, vagy rutinból könnyedén átugrom bizonyos lépéseket, és a mindenható trivialitás égisze alatt azt gondolom, hogy maradéktalanul értem. A szakdolgozatra való készülés során többször ütköztem ebbe: harmadik elemzésre vettem észre, hogy itt még mindig van egy apró részlet, amelyben a miértek még nem tisztázottak számomra sem.

Tanulmányomnak még egy fontos része volt: a kultúr- és matematikatörténeti ,,szösszenetek". Mivel mindhárom téma (a kódolás, a prímszámok és a titkosítás) is komoly történeti, alkalmazási háttérrel bír, így a bőség zavarával kellett szembenéznem, amikor apró történeteket írtam meg sokféle forrást használva. Ezek végül a számrendszerek, irodalmi példák, háborús titkosítások témájából kerültek ki, vagy három nagy magyar matematikust érintenek: Erdős Pált és Neumann Jánost állítják középpontba, Lovász Lászlót szólaltatják meg. Itt egyrészt magyar szakos énem és újságírói tapasztalataim is motiváltak, emellett úgy láttam, hogy az alkalmazásokat, történelmi vonatkozásokat ilyen módon tudom beépíteni. Ugyanis a feladatokkal, a történet folyamával más módon nem alkottak volna koherens egységet. De milyen történetről is beszélek?

1.3. Mese habbal

A választott témáim elindítottak bennem egy gondolatot: kódolásról és kódfejtésről beszélek, ez már önmagában eléggé kalandos. Így egy keretmesére fűztem fel a történetet. A diákok csapata elindul kincset keresni. Az első részben a kincs koordinátáit kell kideríteniük. Ezt követően a kiderített városban várnak rájuk

próbatételek. Majd meg kell szerezni Rejtelmes Sehollakó Anonymustól a jelszót, amihez éppen az RSA-algoritmust kell alkalmazni. Többféle okból döntöttem amellett, hogy történetet körítek a feladatokhoz. Amellett, hogy számomra is izgalmas kihívást jelentett, összefogja a szakdolgozatot. Hiszen így megvan a dramaturgiai mozgatórugó, megvannak a célok, amiért küzdünk. Éppen ezért a diákokat is motiválhatja. Saját magamon tapasztaltam, hogy a különleges elnevezések, az izgalmas történet elvarázsolja az embert, még akkor is, ha hamar látja benne a csupasz matematikát.

Emellett igyekeztem a feladatok többféle tárgyalási stílusát is felvillantani. Van olyan, ahol a mese nem annyira domináns, hanem én magam hozok be alfeladatokat (az első rész), és ezeken keresztül jutunk közelebb a megoldáshoz. Máshol inkább a precízebb leírásra törekszem, és az esetszétválasztás juttat minket célba (második rész). A végén pedig már a csapat tagjai is megszólalnak, és ők lendítik előre a történetet (harmadik rész). Itt Hirtelen Hedvig és Lassúvíz Lajos kerülnek reflektorfénybe. Ugyanis ez a kettősség bennem és nagyon sok diákban is megvan. Azt akartam megmutatni, hogy ez a kettősség jó, előrevivő. Hiszen sokszor a hirtelen ötlet, a gyors észjárás, az ügyesség célravezető. Viszont bizonyos helyzetekben meg kell állnunk, alaposan szemügyre kell vennünk a problémát, és ízekre szedve megoldani, vagy általános érvényű igazságokat keresni. Ilyenkor valóban igaz, hogy lassú víz partot mos.

1.4. A célközönség

Az összeállított anyagot alapvetően egy szakkörre terveztem. Úgy gondolom, hogy érdeklődő, leginkább gimnáziumban tanuló, minimum tizedik évfolyamra járó diákokkal lehet felhasználni a feladatokat. Viszont nem osztottam fel órákra az anyagrészt, mivel a mese folyamát nem akartam megtörni, illetve úgy gondolom, hogy rendkívül diák- és tanárfüggő ennek az alkalmazása. Elképzelhetőnek tartom, hogy bizonyos esetekben csak egy-egy gondolatot, feladatot vennének át a matematikatanárok, máskor akár az egész gondolatiságot.

1.5. Köszönetnyilvánítás

Szakdolgozatomhoz sokan adtak inspirációt. Ezért köszönetet szeretnék mondani Pálfiné Kovács Erikának, aki a Városmajori Gimnáziumban hat éven keresztül megmutatta, hogy miként lehet magával ragadó elánnal beszélni a matematikáról. Ezt idén mentoráltjaként tanári oldalról is tapasztalom, rengeteget segít az elindulásomban. Köszönetet szeretnék mondani Juhász Péternek, aki a ,,Hogyan foglalkozzunk tehetséges gyerekekkel?" elnevezésű speciálkollégium két félévében a felfedeztető tanítás eszmeiségét és fogásait megmutatta. Fontosnak tartom megemlíteni Pósa Lajos, Széchenyi-díjas matematikust, akit a Matematikai Mulatságok Táborában és hétvégi foglalkozásain is láthattam. Csodálatos volt, ahogy lebilincselő módon rendkívül mély matematikai tudással fedezi fel a gyerekekkel együtt ezt az izgalmas világot.

Freud Róbertnek, témavezetőmnek, pedig köszönöm hat éve tartó jelenlétét.

Elsőévesen az ő számelmélet gyakorlata rendkívül meghatározó volt. Vibráló tanári jelenléte, lenyűgöző memóriája, izgalmas feladatai, ,,félelmetes tudása" és a hallgatók iránti elkötelezettsége mintaértékű számomra. Szakdolgozatom készítésekor kreativitásra ösztönzött, miközben végig a matematikai alapokat és módszertani szemléletet tartotta a legfontosabbnak. Amellett, hogy kellő szabadságot hagyott nekem, tudta, hogy mikor kell ösztönzőleg ,,rápirítani" az emberre, hogy valóban elkészüljön a szakdolgozat.

2. A kerettanterv és a szakdolgozat kapcsolata

A kerettantervben megfogalmazott célok, feladatok és követelmények a szakdolgozatomban foglaltakkal egyfajta ,,szimbiózisban élnek". Egyfelől a szakdolgozatom támaszkodik a kerettantervben foglalt követelményekre, bizonyos fogalmak, feladattípusok, módszerek ismeretére, másfelől éppen segíti a tananyag megértését, elmélyítését, de a tananyagon túlmutató, a tanórai keretektől kissé különböző módon. Az alábbiakban röviden összefoglalom, hogy a kerettanterv mely elemeinél jelenik meg ez a kölcsönösség.

Mivel egy tehetséggondozó szakkörre szánom feladataimat, így a matematika szaktárgyi kerettanterv gimnáziumok számára kidolgozott változatát állítottam vizsgálatom középpontjába. A kerettanterv három részre tagolt: Célok és feladatok; Fejlesztési követelmények; valamint a tematikus egységek részletes kifejtése évfolyamokra bontva. E logika szerint fogok én is haladni.

2.1. Célok és feladatok

,,A matematikai nevelés sokoldalú eszközökkel fejleszti a tanulók matematizáló, modellalkotó tevékenységét..." — szerepel a kerettanterv ezen részében. Szakdolgozatomban ez több helyen megjelenik. Például az egyszerű és közismert játékból, a barkochbából kiindulva jutunk el a kettes számrendszerig. Az eldöntendő kérdésre adott igenlő választ 1-gyel, nemleges választ 0-val jelöljük. Hasonlóan járunk el a látszólag ,,ártatlan" kétkarú mérleggel is: kilenc súlyt mérünk le, és hármat az egyik, hármat a másik serpenyőbe teszünk, három pedig az asztalon marad. Mindhárom hely kap egy-egy ,,kódot": 0, 1 vagy 2, és így mérésenként a hely kódszámát a súly mellé írva máris hármas számrendszerbeli alakokat nyerünk; második mérés esetén a második hely kódját az első mögé írva egy kétjegyű hármas számrendszerbeli alakot kapunk és így tovább. A titkosírásoknál hasonlóan megjelenik a modellalkotó tevékenység használata és fejlesztése: a kódolási technikákat függvényeknek tekintjük, a dekódolást pedig a függvény inverzének. Így rögtön felmerül például az invertálhatóság kérdésköre.

,,...megmutatja a matematika hasznosságát, belső szépségét, az emberi kultúrában betöltött szerepét." — A fenti példák már a hasznosságra is rámutatnak. Természetesen a kitűzött feladatok között vannak olyanok, amelyek a köréjük kerített ,,mese" ellenére kissé laborszagúak maradnak, ennek ellenére azt üzenik a diákoknak, hogy a matematikai gondolkodás nagyon sokszor célravezető az életben is. Logikus lépésekkel, a matematika nyelvén fogalmazva gyakran olyan problémákat oldhatunk meg, amelyek elsőre a matematikától nagyon távol esőnek tűnhetnek. De konkrét, nem laboratóriumi példákat is hozok szakdolgozatomban: például a nyílt kulcsú titkosítás részletezése, amely manapság rengeteg intézménynél, például bankoknál jelenti a titkosítás megoldását; illetve történelmi példákon keresztül bemutatom, hogy valóban emberéletek, háborúk múlhattak matematikai alkalmazásokon.

,,Törekedni kell a tanulók pozitív motiváltságának biztosítására..." — Saját tapasztalataim vezéreltek: én magam is sokkal nagyobb lendülettel vetem bele magam egy-egy feladatba, ha egy kis történet, izgalmas kihívás, vagy életszerű helyzet része.

Éppen ezért gondolom úgy, hogy motiválhatja a diákokat, ha egy titkos helyszín koordinátáit kell kitalálni, vagy egy titkosítás megfordításáról gondolkodni.

2.2. Fejlesztési követelmények

,,A problémaérzékenységre, a problémamegoldásra nevelés fontos feladatunk." — Többször nagyobb problémákat vetettem fel, amelyeket utána kisebb lépéseken, alfeladatokon lépkedve oldottunk meg. Ez jól mutatja az életben jelentkező problémák megoldását, vagy a matematikusi munkát: adott egy nagyobb cél, ahova kisebb lépéseket megtéve, például a matematikusok esetén segédállításokon keresztül jutunk el. Illetve nagyrészt olyan feladatokat írtam, választottam, amelyekben a szöveg alapján a diákoknak kellett magát a problémát megfogalmazni, a matematika nyelvén leírni.

,,A logikus gondolkodás a problémamegoldásban, az algoritmikus eljárások során és az alkalmazásokban egyaránt lényeges. A matematika különböző területein néhány lépéses algoritmus készítése az informatika tanulmányozásához is fontos." — A nyílt kulcsú titkosítás részletes bemutatása éppen az algoritmikus gondolkodásmód fejlesztésére is irányul. Kissé bonyolult, több lépésből áll, a matematikai háttere viszonylag összetett, de apró lépésekre lebontva befogadható a diákok számára is. És ha megértették a kisebb gondolatokat, egyet hátraléptek, akkor összeáll bennük az egész eljárás logikája.

,,Komoly motiváció lehet tanításukban a matematikatörténet egy-egy mozzanatának megismertetése, a máig meg nem oldott egyszerűnek tűnő matematikai sejtések megfogalmazása." — Ezt a kitételt rendkívül fontosnak tartom. Tapasztalataim szerint a tananyagot, a tankönyvbe foglalt ,,örökérvényű igazságokat" hajlamosak a diákok steril és unalmas, évezredek óta létező, és évezredek múlva is meglévő ,,dinoszauruszoknak" tekinteni. Holott az emberiség folyamatos fejlődése során jut el egyre újabb és újabb tételekhez, felismerésekhez. Ennek a folyamatnak a nyomon követése, vagy legalábbis kis epizódok ismerete, közelebb vihet minket a megértéshez. Éppen ezért gyűjtöttem kis érdekességeket mind a matematika, mind a történelem, mind a kultúra területéről. Hiszen fontos látni, hogy miként indulnak el gondolatok, vagy miként ütközünk ma, a 21. században is olyan akadályokba, amelyeket még szuperszámítógépekkel sem tudunk leküzdeni.

2.3. A tematikus egységek részletezése

A gimnáziumi matematikaoktatás anyagát öt nagy fejezetben tárgyalja a kerettanterv, évfolyamokra bontva, és ezen egységeken belül elkülönítve fejlesztési feladatokat, tevékenységeket, tartalmat és a továbbhaladás feltételeit. Az öt fejezet: Gondolkodási módszerek; Számtan, algebra; Függvények, sorozatok; Geometria; Valószínűség, statisztika. Az első három témát fogom részletezni, ugyanis ezekkel áll szakdolgozatom szorosabb kapcsolatban.

2.3.1. Gondolkodási módszerek

Egyrészt megjelenik a kombinatív készség fejlesztése, leszámlálási feladatok megoldása. Ezt én is használom, hiszen a barkochbával kapcsolatos feladat ismétléses variációhoz vezet; vagy a relatív prímek leszámlálásánál a logikai szitánál kötünk ki.

Másrészt fontos eleme az ismeretek rendszerezése, a matematika különböző területei közti összefüggések tudatosítása. Például az általam használt számelméleti függvény már önmagában kapcsolatot teremt: oszthatóságról szóló egyértelmű hozzárendelés.

2.3.2. Számtan, algebra

A műveletek végzése és a hatványozás mellett a fent már említett matematikatörténeti vonatkozás itt is megjelenik: ,,A matematika iránti érdeklődés erősítése az elemi számelmélet alapvető problémáival és matematikatörténeti vonatkozásaival." — Tartalmi szinten pedig a relatív prímeket, oszthatósági feladatokat, a prímszámok számát, számrendszereket említi a tanterv. Ezekre én magam is építek, illetve igyekszem erősíteni. A prímekkel esetén például az Erdőssel kapcsolatos érdekességek éppen ötvözik ezeket a törekvéseket.

A felfedezés fontosságát is említik. Ennek magam is híve vagyok, és a szakkör gyakorlati megvalósítása esetén is e szerint járnék el. Nem szabad ,,lelőni a poént", hagyni kell, hogy a tanuló maga keresse például a mérések minimális számát, maga próbáljon a képességeihez mért apró bizonyításokat megoldani.

2.3.3. Függvények

A hozzárendelés szabályként való értelmezése, a megfelelő modell megkeresése, az összefüggések felismerése a matematika különböző területei között mind-mind fontos részét képezik a szakdolgozatomnak. Például célom, hogy a dolgok számokkal való megfeleltetését is egyértelmű hozzárendelésként fogják fel a diákok, vagy lássák a függvényt a titkosítás folyamatában: egy szóhoz hozzárendelünk egy jelsorozatot.

Egyetemi tanulmányaim során azt tapasztaltam, hogy sokszor mereven elkülönülnek bennem a különböző területek. Például a függvényeket sokszor a formalizmus börtönébe zártam magamban, és lényegében csak az elemi függvényekben tudtam gondolkodni, az ,,extrémebbek" esetén megijedtem az újdonságtól. Ezt a gátat szeretném kicsit letörni, és a függvényfogalom kiterjesztésével lazítani a diákokban a fogalom merevségén.

3. Hol van a kincs?

Csapatotok első feladata az volt, hogy kiderítse, pontosan hol található a titkos kincs. Ehhez azonban résen kellett lennetek: hidegvéreteket megőrizve a lehető legjobb megoldásokra volt szükségetek. A következő próbatételek elé állítottak benneteket:

1. *próbatétel: Melyik országban van a kincs?*
2. *próbatétel: Melyik megyében van a kincs?*
3. *próbatétel: A bomba hatástalanítása*
4. *próbatétel: Mik a kincs pontos koordinátái?*

Csak akkor indulhattatok el, ha ezen a négy próbatételen átjutottatok.
Akkor kezdjük el!

3.1. Melyik országban van a kincs?

Azt tudtátok, hogy a világ 50 megadott országának valamelyikében található a kincs. Előre leírt eldöntendő kérdésekkel találhattátok ki az ország nevét, és csupán akkor kaptatok választ, ha a lehető legkevesebb kérdéssel oldottátok meg a feladatot. Mennyi kérdésre volt szükségetek, és pontosan mik voltak ezek a kérdések?

Segítő kérdéseken keresztül a feladat megoldása:

3.1.1. Gondoltam egy számra az 1 és a 2 közül. Hány kérdéssel tudod kitalálni?

Gondolatmenet: 0 kérdés egy szám esetén lenne elég, hiszen akkor az az egy szám lehetne csak a megoldás. Két szám esetén egy kérdésre biztosan szükség van, és egy kérdéssel ki is tudjuk találni. Például: az 1-re gondoltál? Ha igen, akkor az 1 a megoldás, ha nem, akkor a 2.

Megoldás: 1 kérdéssel.

3.1.2. Gondoltam egy számra az 1, 2 és 3 közül. Hány kérdéssel tudod kitalálni?

Gondolatmenet: ismét induljunk ki az egy darab kérdésből. Mivel eldöntendő kérdés, így kétféle választ kaphatunk: igen vagy nem. Ez két részre tudja osztani a meglévő számokat. A skatulyaelv alapján az egyik részben biztosan minimum két szám lesz, hiszen ha mindkét részben maximum egy-egy lenne, akkor az összesen maximum két számot jelentene. Tehát, ha megkérdezzük, hogy: az 1-re gondoltál? Akkor nemleges válasz esetén még nem tudjuk kitalálni, tehát szükséges az a kérdés is, hogy: a 2-re gondoltál? Tehát most ott tartunk, hogy vagy egy, vagy két kérdésre van szükségünk; tehát maximum két kérdéssel ki tudjuk találni. De még nem tartunk pontos számnál, és nem tartunk előre leírt kérdéseknél sem. Ehhez nézzünk meg további feladatokat!

Megoldás: 2 kérdéssel.

3.1.3. Gondoltam egy számra 1 és 4 között. Minimum hány kérdéssel tudod biztosan kitalálni?

Gondolatmenet: az előző logika alapján minden egyes kérdéssel két részre tudjuk osztani a megmaradt számokat. A kérdés az, hogy milyen részekre érdemes osztani. Lehet 1+3 és 2+2 (a 0+4 nyilván kizárható, hiszen akkor egy helyben toporogtunk). Ha az 1+3 felosztást választjuk, akkor az azt jelenti, hogy a kérdésünk egy számra igaz, háromra hamis (vagy lehet fordítva is, egyre hamis, háromra igaz). Például: az 1-re gondoltál? Ekkor nemleges válasz esetén marad három. És az előző feladatban láttuk, hogy ott két kérdés szükséges. Tehát ezzel a taktikával három kérdésből tudjuk biztosan kitalálni. Mi a helyzet a 2+2-es felosztással? Az első kérdés után mindenképpen két szám marad ,,versenyben". Az első feladatban láttuk, hogy itt egy kérdés elegendő. Azaz a 2+2 felállással minden esetben két kérdéssel ki tudjuk találni a számot. Mivel a ,,legrosszabb esetre" is gondolni kell, hiszen biztos kitalálást ígérünk, így a 2+2 felállással érdemes játszani, és ekkor 4 számból két kérdéssel tudunk kitalálni.

Megoldás: 2 kérdéssel.

3.1.4. Mi a helyzet 5, 6, 7, 8, 9 stb. szám esetén?

Gondolatmenet: 5 esetén az 1+4 és a 2+3 felosztások jönnek szóba. 1+4 esetén az esetlegesen megmaradó négy számból 2 kérdéssel tudom kitalálni. Tehát ez esetben 3 kérdés szükséges összesen. 2+3-as felosztás esetén megmaradó 3 számból is 2 kérdéssel tudom kitalálni. Tehát itt mindkét felosztás 3 kérdéshez vezet.

Megoldás: 5 szám esetén 3 kérdéssel.

Gondolatmenet: 6 szám esetén (a nyíl utáni résznél az 1-es az első kérdés, a második szám a megmaradó halmazok közül a nagyobbiknál maximálisan szükséges kérdések száma)

1+5 $\rightarrow$ 1+3 = 4 kérdés
2+4 $\rightarrow$ 1+2 = 3 kérdés
3+3 $\rightarrow$ 1+2 = 3 kérdés

Megoldás: 6 szám esetén 3 kérdés.

7 szám esetén:

1+6 $\rightarrow$ 1+3 = 4 kérdés
2+5 $\rightarrow$ 1+3 = 4 kérdés
3+4 $\rightarrow$ 1+2 = 3 kérdés

Megoldás: 7 szám estén 3 kérdés.

8 szám esetén:

1+7 $\rightarrow$ 1+3 = 4 kérdés
2+6 $\rightarrow$ 1+3 = 4 kérdés
3+5 $\rightarrow$ 1+3 = 4 kérdés
4+4 $\rightarrow$ 1+2 = 3 kérdés

Megoldás: 8 szám esetén 3 kérdés.

9 szám esetén:

1+8 $\rightarrow$ 1+3 = 4 kérdés
2+7 $\rightarrow$ 1+3 = 4 kérdés
3+6 $\rightarrow$ 1+3 = 4 kérdés
4+5 $\rightarrow$ 1+3 = 4 kérdés

Megoldás: 9 szám esetén 4 kérdés.

Először azt érdemes észrevenni, hogy mely felosztások célravezetők. Az adott mennyiséget kétfelé bontjuk, és a nagyobbik halmaznál vizsgáljuk a kérdések számát (hiszen több szám esetén a kérdések száma is nagyobb vagy egyenlő). Ezért páros szám esetén: $2k$ db számból $k+k$ felosztással tudjuk a legkevesebb kérdéssel biztosan megkapni a választ (hiszen, ha az összeg valamelyik tagja kisebb, mint k, akkor a másik tag értelemszerűen nagyobb, mint k; így azzal a felbontással nagyobb vagy egyenlő kérdésre lenne szükség). Hasonló logikával páratlan szám esetén: $2k+1$, ekkor $k+(k+1)$ a legjobb felbontás. Ezen logika szerint ha $2k$ db számhoz tartozó minimum kérdésszám B_{2k}, akkor azt elmondhatjuk, hogy $B_{2k} = B_k + 1$. Erre majd visszatérünk. Vizsgáljuk meg, hogy 1-től 9-ig milyen értékeket kaptunk:

k:	1	2	3	4	5	6	7	8	9
B_k:	0	1	2	2	3	3	3	3	4

Hol változnak a számok? Láthatjuk, hogy a váltás 1, 2, 4 és 8 után van. Ha tovább számolunk, akkor láthatjuk, hogy a következő váltás 16, az azt követő 32 után következik. Mi a közös ezekben a számokban? Egymást követő kettőhatványok. Mi lehet ennek az oka?

Ha van egy darab kérdésem, akkor az két dolgot tud megkülönböztetni. Ha van két darab kérdésem, akkor az elsőre is kétféle, a másodikra is kétféle válasz adható. Ezek függetlenek egymástól, azaz négy dolgot tud egymástól megkülönböztetni: igen-igen, igen-nem, nem-igen, nem-nem válaszokkal. Három kérdés esetén szintén kétféle válasz adódik minden kérdésre, azaz, ha az igen-nemeket leírjuk, akkor az első helyre is kétféle válasz kerülhet, a másodikra és a harmadikra is, azaz ekkor $2 \cdot 2 \cdot 2 = 8$ különböző variációja létezik a válaszoknak. Ha n darab kérdésünk van, akkor is minden kérdés kétféle kimenetelű lehet, ugyanúgy függetlenek, azaz n darab kettest kell összeszoroznunk: $2 \cdot 2 \cdot ... \cdot 2 = 2^n$ dolgot tudunk maximum megkülönböztetni vele.

Azaz $n-1$ kérdéssel maximum 2^{n-1} dolgot tudunk megkülönböztetni, n kérdéssel pedig maximum 2^n dolgot. Azaz kettőhatványok esetén tisztán látszik, hogy ahány kettes tényezőből áll, annyi darab kérdésre lesz szükség. De mi a helyzet nem kettőhatványok esetén? A táblázat alapján is láthatjuk, illetve a fentiekből logikusan következik, hogy: ha l esetén $2^{n-1} < l < 2^n$, akkor l darab számból legkevesebb n darab kérdéssel tudjuk biztosan kitalálni a gondolt számot.

Az 1. próbatétel megoldásának 1. része: Ezek alapján a kérdés első részére tudjuk a választ. Hiszen 50 országról van szó, így mivel $32 < 50 < 64$, azaz $2^5 < 50 < 2^6$, ezért 50 dolog esetén 6 kérdésre lesz szükség. Viszont azt még nem tudjuk, hogy előre leírt kérdésekkel hogyan tudunk dolgozni, hiszen eddig a

válaszok alapján gondolkodtunk (azaz, ha az első kérdésre nemleges válasz érkezett, akkor tudtuk, hogy a megmaradó számokból kell kitalálnunk). Ezt vizsgáljuk meg a továbbiakban.

3.1.5. Gondoltam egy számot 1 és 4 között. Legkevesebb hány darab előre leírt kérdéssel tudhatjuk meg a választ?

Gondolatmenet: azt tudjuk, hogy minimum két kérdés kell, hiszen nem előre leírtak esetén is ennyire van szükség. Az előre leírtak esetén az a lényeg, hogy a két kérdésre adható variációk egyértelműen egy-egy számot határozzanak meg. Azaz például az igen-igen az 1-et, az igen-nem a 2-t, a nem-igen a 3-at, a nem-nem pedig a 4-et jelentse. Például ennél a megfeleltetésnél: 1. kérdés: Kisebb mint 3?, 2. kérdés: Páratlan szám?

	1. kérdés igen	1. kérdés nem
2. kérdés igen	1	2
2. kérdés nem	2	4

Megoldás: Azaz két darab előre leírt kérdéssel megválaszolható. De mi a helyzet több szám esetén? Milyen általános kérdés segíthet mindig? Erre nézünk példát a következő feladattal.

3.1.6. Gondoltam egy számot 1 és 2^n között. Legkevesebb hány darab előre leírt kérdéssel tudhatjuk meg a választ?

Gondolatmenet: az előző feladatok alapján láthatjuk, hogy n darab kérdés minimum szükséges. Kérdés, hogy elég-e. A 4 számból való kitalálásnál már megfeleltettük a lehetséges válaszsorozatokat egy-egy számnak. Ez n darab kérdés esetén például így néz ki: igen-igen-igen-igen-...-igen-től a nem-nem-...-nem-ig van 2^n darab válaszsorozatunk, ezeket egyértelműen meg akarjuk feleltetni az 1-től 2^n-ig terjedő számoknak. Jó volna valamilyen logika alapján tenni ezt: kisebb számhoz ,,kisebb" válaszsorozatot. De ez hogyan lehetséges? Mit jelent az, hogy egy válaszsorozat kisebb?

Mivel kétféle válaszunk van, így ezt a kétféle választ érdemes egy-egy számmal helyettesíteni. Mivel az igen azt jelenti, hogy teljesül, így az lehet az 1-es, a nem azt jelenti, hogy nem teljesül, az lehet a 0. Így láthatjuk, hogy 0-kból és 1-ekből álló n hosszú számsorokat eredményeznek a válaszsorozatok.

Honnan lehetnek ismerősek ezek a számsorok? Miféle módon feleltettük meg ezeket a számsorokat a számainknak? Könnyen adódik, hogy ezek a számsorok a számok kettes számrendszerben felírt alakjai. Mivel 2^n darab számunk van, a 0-ból és 1-ből álló sorozat n darab tagból áll, és $2^n - 1$-ig minden számot felír kettes számrendszerben, plusz a 0-t, így adódik a megfeleltetés:

$1 \quad \rightarrow \quad 000...001$
$2 \quad \rightarrow \quad 000...010$
...
$2^n - 1 \quad \rightarrow \quad 111...111$
$2^n \quad \rightarrow \quad 000...000$

Látható, hogy a válaszsorozatok és az 1-től 2^n-ig terjedő számok között kölcsönösen egyértelmű megfeleltetést létesítettünk. Már csak azt kell tisztáznunk, hogy milyen előre leírt kérdésekre van szükség. Mivel például az 1-es esetén is n darab számjegyről van szó (a kettes számrendszerbeli alakja elé $n-1$ darab 0-t írtunk), így mindenhol n darab helyi értékhez rendeltünk számokat, 0-t vagy 1-et. Tehát, ha helyi értékenként kérdezünk rá a kigondolt számra, akkor az első kérdésre adott válasz nem befolyásolja a második kérdést és így tovább.

Megoldás: Tehát a kérdéseink: a kigondolt szám kettes számrendszerbeli alakjának 1., 2., ... , n. helyi értéken álló számjegye 1-es? És így az n kérdésre kapott válaszok után egyértelműen meg tudjuk határozni az adott számot.

Az 1. próbatétel megoldásának 2. része: Az előzőek logikája alapján tehát hamarosan fel tudjuk írni a szükséges kérdéseket. Ehhez két dolgot kell tisztázni:

1. Mi a helyzet, ha nem kettőhatvány darabszámú dologból kell kitalálnunk?
2. Mit tehetünk, ha országokról, és nem számokról van szó?

Az előzőekben láthattuk, hogy ha nem kettőhatványról beszélünk, akkor meg kell keresnünk a hozzá legközelebb álló, nála nagyobb kettőhatványt, jelen esetben ez a 64. Azaz 6 kérdésre lesz szükségünk. Ugyanúgy, ahogy 2^n-nél tettük, itt is a számok kettes számrendszerbeli alakját kell felírnunk. Itt annyi a különbség, hogy bizonyos válaszsorozatokhoz nem tartozik majd érték, például 50 esetén az 111111 érvénytelen lesz, hiszen a 63 nem lehet megoldás.

A második kérdés pedig könnyen orvosolható: az 50 országot bármilyen logika alapján, például ábécé szerint, sorba rendezhetjük, és a sorszámokat feleltethetjük meg az országoknak. Például Albánia lesz az 1-es. Tehát a megoldás: Az országokhoz rendelt számok kettes számrendszerbeli, 0-kkal kiegészített alakjának 1., 2., 3., 4., 5. és 6. helyi értéke 1-es?

Matematikai általánosítás: Lehetséges értékek: $1, 2, ..., n$. Eldöntendő kérdéseket tehetünk fel. Ekkor $\lceil \log_2 n \rceil$ darab kérdésre van szükség.

3.1.4. esetén írtuk: $B_{2k} = B_k + 1$.

Most beláthatjuk:

B_k: k darab szám esetén, ha $2^{n-1} < k \leq 2^n$, akkor n darab kérdésre van szükségünk. Ezt az egyenletet 2-vel megszorozzuk: $2^n < 2k \leq 2^{n+1}$-t kapjuk, azaz:

$B_{2k} = n + 1 \rightarrow$ az állításunk igaz volt.

Érdemes meggondolni, hogy $3, 4, ..., n$-féle kimenetellel rendelkező kérdések esetén hogyan gondolkodhatunk.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

Tudtad-e? Bár Kohba és Karinthy Frigyes története

Bár Kochba a zsidó nép utolsó szabadságharcának vezére volt i.sz. 131-135-ben. Eredeti neve Bár Koziba vagy Bar Koseba, hívei nevezték el Bár Kochbának, jelentése a Csillag Fia, ugyanis egyfajta messiásként tekintettek rá. Azt homály fedi, hogy a játék és a személy között milyen összefüggés lehet, ugyanis ez az elnevezés magyar sajátosságnak tűnik, angolul például Twenty Questions-nek hívják. Kuczka Péter *A szórakozás értelme* című tanulmányában így ír a kapcsolat lehetséges eredetéről:

,,Mindkét történetet Karinthy Frigyes ,,jegyezte le", de arra, hogy ő találta ki, nincsen bizonyítékunk. Egyszer állítólag tiltakozott is az ellen, hogy a játék elnevezése tőle származna. Annyi azonban biztos, hogy forrásokra sehol sem hivatkozott és játékos természetét ismerve jogosan hihetjük, hogy nem feledékenységgel, hanem tréfával, misztifikációval van dolgunk. Később a történet két alaptípusának változataival is találkozunk, ezek azért fontosak, mert legtöbbször a játék alapszabályainak kisebb-nagyobb módosítását is tartalmazzák.

Az első történet szerint Bár Kochba éppen bíráskodott, amikor egy emberi roncsot vittek elébe. Keze, lába le volt vágva, szemét kiszúrták, nyelvét, száját szétmarta valami sav. Eszméletén volt, de látszott, hogy utolsó óráit éli. (Jegyezzük meg ezt a mondatot, később még visszatérünk jelentőségére.) Bár Kochba kérdezni kezdett és bár az ember csak igent vagy nemet tudott bólintani, sikerült fényt deríteni a borzalmas bűntényre. A szerencsétlen férfi elárulta feleségének családja titkát, egy aranybánya helyét. Az asszony szeretőjével együtt fosztogatni kezdte a bányát, aztán megszökött. A férfi testvérei rájöttek a dologra és bosszút álltak az esküszegőn. Bár Kochba kiszedte az emberi roncsból még a nevét is, aztán elfogatta és elítélte a bűnösöket.

A másik monda másik változatában Bár Kochba felderítőt küldött a rómaiak táborába. Az ellenség elfogta a felderítőt, megcsonkította, nyelvét is kivágta, majd visszavitette övéihez. (Egyik változat szerint ,,visszaszökött", dehát ez csak elírás lehet.) A felderítő mindent tudott a rómaiak erejéről, terveiről, tehát ott voltak fejében a szükséges információk, de hozzáférhetetlenül. Az okos és bölcs vezér megoldotta a problémát. Ügyes és logikus kérdéseivel, melyekre a beszélni nem tudó ember igent vagy nemet intett, mindent megtudott a rómaiak erejéről." (Kuczka 2011)

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

3.2. Melyik megyében van a kincs?

A kapott válaszok alapján kiderült, hogy Magyarországon van a kincs. Most azt kellett kiderítenetek, hogy a fővárosban, vagy a 19 megye valamelyikében rejtették-e el. Ismét előre leírt kérdésekkel kellett dolgozni. Ám a válaszlevél útközben kinyílt, és a külön cetliken szereplő válaszok

egyike elveszett. Most hány kérdésre volt szükség? Mik lehettek ezek a kérdések?

(Azt tudjuk, hogy melyik válasz melyik kérdésre érkezik, tehát tudjuk, hogy melyik válasz hiányzik.) (Juhász 2010)

Segítő kérdéseken keresztül a feladat megoldása:

3.2.1. Mi a megoldás, ha nem vész el egy válasz sem?

Gondolatmenet: Erre a kérdésre az előzőek alapján könnyen adódik a válasz: $16 < 20 < 32$, így 5 kérdésre lesz szükség, és az előzőekhez hasonlóan a kettes számrendszerbeli 0-kal kibővített alakokra kérdezünk rá.

Megoldás: 5 kérdésre lesz szükség.

3.2.2. Mi a megoldás, ha csak 8 dologból kell kitalálni, és úgy vész el egy válasz?

Gondolatmenet: Mi a kézenfekvő ötlet? Mindent kétszer kérdezünk meg, így bármelyik is vész el, akkor van egy tartalék. Ám ez igencsak pazarlónak tűnik, bizonyára találunk ennél ,,spórolósabb" megoldást is. Azt láthatjuk, hogy a 8 esetén adódó 3 kérdés nem lesz elég, hiszen ha egy elvész, akkor a maradék 2 válasszal legfeljebb 4 dolgot tudunk kódolni. Azaz minimum még egy kérdésre szükség van. De mivel is szembesülhetünk az elveszett válasz esetén?

Például:

1...0	$\rightarrow$	ez eredetileg lehetett 110 és 100 is
...01	$\rightarrow$	ez eredetileg lehetett 101 és 001 is
01...	$\rightarrow$	ez eredetileg lehetett 011 és 010 is

A változatok milyen általános dologban különböznek? A benne szereplő számjegyek összegének paritása nem ugyanaz. És ez általános érvényű.

A 2. próbatétel megoldása: Eredetileg 5 kérdésre volt szükségünk. Ám most 6. kérdésként fel kell tennünk: a válaszban szereplő számjegyek összege páratlan? Ez működni fog, hiszen ha az utolsó válasz vész el, akkor a szokásos módon gondolkodunk; ha valamelyik számjegyünk veszett el, akkor a megmaradókat összeadjuk, és a paritásra adott válasz alapján vagy 0-t, vagy 1-et írunk az üresen maradó helyre.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

Tudtad-e? A számrendszerek

A hatvanas számrendszert és a helyi értékek bevezetését a babiloniaknak köszönhetjük. Ékírásos jelekkel írták le a számjegyeket, ám nem volt 59 különböző jelük, hanem csupán kettő: egy lefelé szűkülő ék és egy balra mutató nyíl feje. Ezekkel tudtak mindent leírni: ahány tízes, annyi nyíl, ahány egyes, annyi ék, egészen hatvanig, amikor is a hatvan megint egy ék (azaz ugyanúgy, mint az egyes), csak a helyi értékétől függött, hogy ez 1, 60, 60^2, vagy 60^3 és így tovább. Viszont se nullát, se tizedesvesszőt nem használtak, így ha csupán egy éket látott az ember, akkor a szövegkörnyezetből kellett kikövetkeztetni, hogy ez a 60 melyik hatványát is jelenti. (Markó 1996)

Habár már a maja kultúrában jelölték a nullát számjegyként (kagyló jellel) a 3. század körül, feltételezéseink szerint először a 6. század talán legkiválóbb indiai matematikusa, Brahmagupta tekintette matematikai értelemben is számnak. A verses formában megírt húszkötetes művében többek között az előjeles számok műveleti szabályait ismerteti (a pozitív számok a vagyont, a negatívok az adósságot jelentették), illetve a nullával végzett műveleteket igyekezett definiálni, bár néhol rosszul (például a nullával való osztás esetén). (Simon)

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

3.3. A bomba hatástalanítása

Sikerült kideríteneteknek, hogy Budapesten van a kincs! Ám kétséges volt, hogy eljuttok-e oda, ugyanis hatalmas veszélyben voltatok. Ezer éve éppen alattatok ástak el egy bombákkal teli ládát. Ebben 9 darab bomba volt található, melyekre sorra 101, 102,..., 109 gramm volt írva. Közülük 8 valóban annyit nyomott, viszont egyikük egy kicsit többet. Ez az egy robbanhatott fel hamarosan. Hogyan tudtátok egy kétkarú mérlegen, előre leírt mérésekkel leggyorsabban megállapítani, hogy melyik robbanhat? (Juhász 2010)

Segítő kérdéseken keresztül a feladat megoldása:

3.3.1. Van 9 darab bombánk, 8 közülük azonos tömegű, viszont egy darab kicsit nehezebb. Milyen méréseket végezzünk egy kétkarú mérlegen? (Nem szükséges előre leírtakat csinálni.)

Gondolatmenet: a kétkarú mérleg arról ad információt, hogy a bombák három csoportjából (a mérleg egyik és másik serpenyőjében lévő bombák csoportja, illetve a kimaradó bombák csoportja) melyikben található a keresendő darab. Tehát a barkochbához hasonlóan csoportokra tudjuk osztani a 9 darabunkat, és egy mérés után már csak egy csoporton belül kell méréseket végeznünk.

Mivel a ,,legrosszabb" esettel, azaz a legnagyobb csoport megmaradásával kell számolnunk, így úgy kell három csoportra osztani a bombákat, hogy a lehető legkisebb legyen a maximális csoportban lévő bombák darabszáma. Ez mindig $\lceil \frac{n}{3} \rceil$ lesz. Jelen esetben a 3-3-3 felosztás lesz ideális (a két csoportra osztás logikájához hasonlóan ez is végiggondolható).

Tehát 3-3 bombát a két serpenyőbe teszünk, 3 pedig marad a helyén. Ha a serpenyők nem egyenlítik ki egymást, akkor abban a csoportban van a bomba, amelyik lejjebb van, ha kiegyenlítik egymást, akkor abban, amelyik kimaradt. A második mérésben az adott csoport három bombájából egyet az egyik, egyet a másik serpenyőbe teszek, a harmadikat kint hagyom. Ekkor egyértelműen kiderül, hogy melyik a nehezebb. Azaz két mérésre volt szükségünk.

3.3.2. Van 9 darab bombánk, 8 közülük azonos tömegű, viszont egy darab kicsit nehezebb. Milyen méréseket végezzünk egy kétkarú mérlegen, ha előre le kell írni a méréseket? (Azaz, hogy melyik bomba mikor hol van a mérés alatt.)

Gondolatmenet: azt láttuk, hogy nem előre leírt mérésekkel két mérés elegendő. Illetve azt is láthattuk, hogy egy kérdésre most háromféle válasz adódik: egyik serpenyő, másik serpenyő, kimaradók.

Tehát a bombákat is háromféle helyre pakolhatjuk, a lényeg, hogy semelyik két bomba se legyen az első és a második mérés során is egy serpenyőben (hiszen, ha mindkétszer az a nehezebb, akkor nem fogjuk tudni, hogy a kettő közül melyik a nehezebb). Tehát a következő elhelyezés például jó lehet:

Első mérés:		**Második mérés:**	
1. serpenyő:	1., 2., 3.	1. serpenyő:	1., 4., 7.
2. serpenyő:	4., 5., 6.	2. serpenyő:	2., 5., 8.
3. kimaradók:	7., 8., 9.	3. kimaradók:	3., 6., 9.

Azaz más megfogalmazásban:

1	2	3
4	5	6
7	8	9

Ezt a táblázatot soronként és oszloponként is lemérjük (így jól látszik, hogy semelyik kettő nem lesz a két mérés alatt kétszer is ugyanabban a serpenyőben).

A 3. próbatétel megoldása: Az azonos tömegű bombákhoz hasonlóan itt is arra kell figyelni, hogy két egymást követő mérésben semelyik kettő ne legyen kétszer azonos serpenyőben. Emellett viszont még van egy fontos kitétel: itt a tömegek összegére is figyelni kell. Kérdés: így is megadható két mérés, amelyek minden feltételnek megfelelnek?

Ehhez először meg kell tudni, hogy egy serpenyőben összesen mekkora össztömegre lesz szükség. A bombák összesen $101 + 102 + ... + 109 = 945$ grammosak, azaz egy serpenyőbe 315 g kell.

Rövid próbálkozás után például ezt a felállást találhatjuk:

101, 109, 105 | 106, 102, 107 | 108, 104, 103

Ekkor kezdjük el ezeket szétszedni, mindegyik serpenyőből vegyünk egyet-egyet, így ezt kapjuk:

101, 106, 108 | 109, 102, 104 | 105, 107, 103

Így találtunk olyan mérést, amely előre leírt, és csupán két mérés szükséges hozzá.

Matematikai általánosítás: a barkochbához hasonlóan itt is lehet általános képletet adni a szükséges kérdések (mérések) számáról. Mivel három válaszlehetőség van, így 3^n dolgot különböztethetünk meg n darab kérdéssel. De mi a helyzet, ha a megkülönböztetni kívánt dolgok száma nem háromhatvány? Ahogy a barkochbánál láthattuk, ilyenkor azt kell megvizsgálni, hogy melyik két háromhatvány közé esik. Például tekintsük az 50-et! Azt tudjuk, hogy $27 < 50 < 81$, azaz $3^3 < 50 < 3^4$. Mi derül ki ebből? 3 méréssel legfeljebb 27 dolgot tudunk megkülönböztetni, 4 kérdéssel pedig legfeljebb 81-et. Mivel csak egész lehet a mérések száma, így 50 esetén 4-re lesz szükség, hiszen 3 kevés lenne (nem jutna minden dolognak külön ,,kód"). Ennek értelmében x dolog esetében $\lceil \log_3 x \rceil$ felsőegészrész mennyiségű kérdésre van szükség. Komoly nehézségekhez vezethet, ha a súlyok összege nem osztható hárommal, de erre bővebben nem térünk ki.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

Tudtad-e? Az agy és a számológép

A vegyészmérnöki diplomát is megszerző Neumann János a fenti címmel írt, befejezetlenül maradt könyvének bevezetésében így fogalmaz: ,,Azt gyanítom, hogy az idegrendszer mélyrehatóbb matematikai — a fentebb körülírt értelemben »matematikai«— vizsgálata kihatással lesz arra is, ahogyan magának a matematikának e vizsgálódásban közrejátszó oldalait értelmezzük. Sőt talán még a tulajdonképpeni matematikáról és logikáról alkotott képünk is módosulni fog. Később igyekszem majd megmagyarázni, hogy miért hiszem ezt." (Neumann 1972) Marx György elmondása szerint a számítógépet az élő sejt metaforájának tekintette. Így fontos törekvése volt az agy működésének megértése, például az idegrendszer kettős, digitális és analóg működését is vizsgálta (Czeizel 2011: 296): ,,Észrevételeim a következők: Az idegrendszeren áthaladó folyamatok — amint erre már korábban rámutattam — jellegüket ismételten digitálisról analógra és analógról digitálisra változtathatják. Például a folyamat egyik szakaszát — mondjuk bizonyos izom összehúzódását vagy egy meghatározott vegyi anyag kiválasztását — idegimpulzusok irányíthatják, s ezek a mechanizmus digitális részébe tartoznak. Az említett jelenségek maguk (az izomösszehúzódás, az anyagkiválasztás) már az analóg osztályba

tartoznak, de kiindulópontul szolgálhatnak egy újabb idegimpulzus-sorozat számára, amelyet e jelenségeknek a megfelelő belső receptorok által való érzékelése vált ki." (Neumann 1972)

Apró érdekesség: kutyáját Inverznek hívták, ugyanis amikor megérkezett hozzájuk az újdonsült kedvenc, akkor Neumann éppen az inverz függvényekkel foglalkozott. (Czeizel 2011: 275)

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

3.4. Mik a kincs pontos koordinátái?

A ládát kiásva a bombát szerencsésen hatástalanítottátok, így a viharfelhőket egyelőre elfújta a szél. Viszont újabb nehézségbe ütköztetek. A kincs pontos koordinátáit csapatotok egyik fele táviratban akarta elküldeni a többieknek. Ehhez előre meg kellett beszélni, hogy hogyan fogják kódolni a kapott számokat, ha csupán egy billentyűjük van, az 1-es (azt bármennyiszer lenyomhatják), de nem tudják, hogy hány darab és mekkora számot fognak kapni. Mi a célravezető taktika? (Juhász 2010)

Segítő kérdéseken keresztül a feladat megoldása:

3.4.1. Mi a helyzet, ha a 0, 1, 2,..., 9 számjegyeket mind használhatom?

Ilyenkor a számok leírása nem okoz gondot, csupán az elválasztásuk. Mivel nem tudjuk előre, hogy milyen számokat kapunk, így trükközni sem tudunk: ha abban maradunk, hogy 3 darab 0-val választjuk el a számokat, akkor elképzelhető, hogy kudarcot vallunk, hiszen lehet valamelyik számon belül 3 darab 0. Így azt kellene elérni, hogy valamelyik számjegy ,,felszabaduljon", és vesszőként funkcionálhasson. Például szabadítsuk fel a 9-est! Hogyan tudnánk ehhez átírni a számokat? Mi az a felírási mód, amely csak a 0, 1,..., 8 számjegyeket használja?

Megoldás: A kilences számrendszer. Így, ha átírjuk kilences számrendszerbe a kapott számokat, és a 9-est elválasztóként használjuk, akkor kódolni tudjuk az üzenetet. Ezt egészen három billentyűig használhatjuk: kettes számrendszerben felírjuk a számokat, és a 2-es lesz az elválasztó.

3.4.2. Mi a helyzet, ha csak a 0 és az 1 számjegyeket használhatom?

Ekkor az egyiket mindenképpen elválasztóként kell használnunk, a másikkal kell az adott számokat jelölni. Például legyen a 0 az elválasztó. Hogyan tudom az 1-essel a számokat felírni? Például az 534-et hogyan tudom az 1-essel felírni? 534 darab 1-es írásával egyértelműen jeleztem.

A 4. próbatétel megoldása: Egészen 2 darab billentyűig eljutottunk. Azt láttuk, hogy egy konkrét számot fel tudunk írni csupán 1-esekkel. A 3.4.1. feladatban a kapott számokat hogyan kódoltuk? Egy számsor volt az egész. Tehát értelmezhetjük egy darab számként is: azaz felírunk annyi darab 1-est, amennyi a

szám értéke. Például, ha az üzenet 23, 45, 256, akkor ezeket a számokat felírom 9-es számrendszerben: $25_9, 50_9, 314_9$. Ezeket a 9-essel tudom elválasztani, így az üzenet: 259509314. És amikor csak 1-est használhatok, akkor 259509314 darab 1-est kell küldenem.

Megérkezett az üzenet a többiektől. Megtudtátok a kincs pontos koordinátáit. Így nekivághattatok a nagy kincskeresésnek. Ám fel kellett készülnetek a nem várt akadályokra. Egyetlen fegyveretek pedig az eszetek!

4. A rejtelmes város

Kezetekben vannak a titkos koordináták. Ám az út továbbra sem volt egyszerű. Az elkövetkező 5 próbatétel is rendesen megdolgoztatta az agyatok. Prímszámokról kellett gondolkodnotok az alábbi feladatokban:

5. próbatétel: A príma kapukód

6. próbatétel: A kőbe vésett egyenlet

7. próbatétel: A szórakozott öregurak

8. próbatétel: Ne légy racionális!

9. próbatétel: A prímallergia

Szerencsére nem feledtétek, hogy a matematikában mindig jól jön egy kis alaposság, az esetek szétválasztása! A lényeg, hogy sose ijedjetek meg a próbáktól!

4.1. A príma kapukód

Budapestre érkeztetek. De csak akkor juthattatok be a városkapun, ha helyesen adtátok meg a szükséges kódot. A kódról a következőt tudtátok: Két prímszám, melyek különbsége 100, tízes számrendszerbeli alakját egymás mögé írva egy újabb prímszámot kaptok. Melyek ezek a számok? (Róka 2006: 33.)

Segítő kérdéseken keresztül a feladat megoldása:

Induljunk el az elején!

$p = 2$ esetén már a $p + 100 = 102$-nél elakadunk, hiszen $102 = 2 \cdot 51$ összetett szám.

$p = 3$ esetén $p + 100 = 103$ prím, $\overline{p(p+100)} = 3103 = 29 \cdot 107$ összetett szám, viszont $\overline{(p+100)p} = 1033$ prímszám, azaz megfelel a feltételnek. De találunk-e még ilyet?

$p = 5$ esetén $105 = 3 \cdot 5 \cdot 7$ összetett szám.

$p = 7$ esetén 107 prím, de $7107 = 3 \cdot 23 \cdot 107$ és $1077 = 3 \cdot 359$

$p = 11$ esetén $111 = 3 \cdot 37$

Tehát eddig a $p = 3$ volt az egyetlen megoldás. Min bukott el a többi prím? Vagy az egyik, vagy a másik "gyártott" számról bebizonyosodott, hogy összetett. Mi volt az a prímtényező, amelyik mindegyikben szerepelt?

Ez a 3. Mi lehet ennek az oka? Milyen prímeket kellene vizsgálnunk ahhoz, hogy a „gyártott" számok ne legyenek 3-mal oszthatók?

Először is nézzük meg, hogy $a + 100$ mit jelent. Mivel a 100 hármas maradéka 1, így p hármas maradéka csak 0 és 1 lehet, különben a $p + 100$ osztható volna 3-mal (lásd: $p = 5$, $p + 100 = 105$).

Ha a p hármas maradéka 0, az csak a $p = 3$ esetben lehet, amit már megvizsgáltunk. Ha p hármas maradéka 1, akkor $p + 100$ hármas maradéka 2. Mennyi lesz $\overline{p(p+100)}$ és $\overline{(p+100)p}$ hármas maradéka? Mivel a hármas maradék a számjegyek összegétől függ és az így kapott számok számjegyeinek összege alapján számolt hármas maradék $1 + 2 = 2 + 1 = 3$, így minden $3k + 1$ alakú p esetén a számok egymásutánjával keletkezett számok 3-mal oszthatók lesznek.

Azaz az egyedüli megoldást a $p = 3$ adja.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

Tudtad-e? Közösségi prímvadászat

Mind a matematikusokat, mind az érdeklődő laikusokat kíváncsi izgalommal tölti el a prímek keresése. A Nagy Internetes Mersenne–Prímszám Kutatás (GIMPS) mindenki számára nyitott: csupán számítógépe szükséges a bekapcsolódáshoz. Itt Mersenne–prímeket, azaz $2^p - 1$ alakú prímeket keresnek, ahol p prím. Az eddigi utolsót, a 47. találatot 2009. április 12-én lőtték, ám a jelenleg ismert legnagyobb Mersenne–prím a 45. megtalált szám, 2008. augusztus 23-án ,,látott napvilágot" 12978189 számjeggyel, ő a $2^{43112609} - 1$ névre hallgat. (Weisstein 2009)

Máig megoldatlan, hogy vajon végtelen sok Mersenne–prím létezik-e, jelenlegi feltételezések szerint igen. Ehhez hasonló a Fermat-prímek problémája, azaz, hogy létezik-e végtelen sok $2^{2^n} + 1$ alakú prím. Fermat azt gondolta, hogy ez minden n-re prímet ad, ám ezt 1732-ben a 25 éves Euler megcáfolta, ugyanis belátta, hogy az $F_5 = 2^{32} + 1$ osztható 641-gyel. A tudomány jelenlegi állása szerint azt tudjuk, hogy $0 \leq n \leq 4$ esetén F_n valóban prím, ám 5 és 32 között bizonyítottan összetett szám. Eddig nem találtak olyan 4-nél nagyobb n-t, amelyre F_n prím, éppen ezért itt a feltételezések szerint nem is fognak több Fermat–prímet találni. A számelmélet és a geometria között kapcsolatot teremtő, a Fermat–prímekről szóló érdekes tételt Gauss mondta ki: egy szabályos N-szög akkor és csak akkor szerkeszthető (euklideszi szerkesztéssel), ha N kanonikus alakja $N = 2^\alpha \cdot p_1 \cdot p_2 \cdot ... \cdot p_r$, ahol a p_i számok különböző Fermat-prímek. (Freud – Gyarmati 2006: 158–166)

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

4.2. A kőbe vésett egyenlet

A kapun átjutva a kőbe vésve ezt az egyenletet találtátok:

$$[a; b] + (a; b) = a + b + p$$

Csak akkor nyerhettetek bebocsátást a városba, ha kitaláltátok, hogy a betűk milyen számokat rejtenek, ha azt tudjátok, hogy a, b pozitív egészek és p prím. (Kosztolányi – Kovács – Pintér – Urbán – Vincze 2007: 70)

Segítő kérdéseken keresztül a feladat megoldása:

Érdemes először p paritását megvizsgálni a és b függvényében:

I. eset: a, b is páros $\rightarrow [a;b]$ és $(a;b)$ is páros , tehát az összegük is páros, ahogy $a+b$ is páros $\rightarrow p$ is páros $\rightarrow p=2$.

II. eset: a, b is páratlan $\rightarrow [a;b]$ és $(a;b)$ is páratlan, tehát az összegük páros, ahogy $a+b$ is páros $\rightarrow p$ páros $\rightarrow p=2$.

III. eset: a páros, b páratlan $\rightarrow [a;b]$ páros és $(a;b)$ páratlan $\rightarrow [a;b]+(a;b)$ páratlan, $a+b$ is páratlan $\rightarrow p$ páros $\rightarrow p=2$.

Tehát p minden esetben 2.

Ennek fényében az egyenletünk így néz ki:

$$[a;b]+(a;b)=a+b+2$$

A legkisebb közös többszörös és a legnagyobb közös osztó esetén fontos megvizsgálni a relatív prím esetet, így először ezzel kezdjük:

I. eset: a és b relatív prímek $\rightarrow [a;b]= a\cdot b$ és $(a;b)=1$. Tehát az egyenletünk így néz ki:

$$a\cdot b+1=a+b+2$$

Ezt b-re rendezzük:

$$b=\frac{a+1}{a-1}=1+\frac{2}{a-1}$$

Mivel a és b pozitív egészek, így $a-1=1$, vagy $a-1=2$. Ha $a-1=1$, akkor $a=2$ és $b=3$, ha $a-1=2$, akkor $a=3$ és $b=2$, ezek ugyanazt az esetet jelentik, hiszen a és b szerepe szimmetrikus az egyenletben.

Ellenőrzés: $[2;3]+(2;3)=6+1=7$ és $2+3+2=7$, tehát egy megoldást találtunk.

II. eset: a és b nem relatív prímek: legyen k a legnagyobb közös osztójuk:

$$a=k\cdot n,\quad b=k\cdot m,\quad (n;m)=1$$

Ekkor így néz ki az egyenletünk:

$$k\cdot n\cdot m+k=k\cdot n+k\cdot m+2$$

Átrendezve:

$$k(n\cdot m-n-m+1)=2$$

a) eset: $k=1\rightarrow$ visszavezettük a relatív prím esetre.

b) eset: $k=2$

$n\cdot m-n-m+1=1$

$n=1+\frac{1}{m-1}$

Az n és m pozitív egészek, így $m-1=1$, azaz $m=2$, $n=2$, $a=4$, $b=4$. Ellenőrzés szerint: $8=10$, ami ellentmondás, tehát ez nem megoldás. (Ez már abból is kiderült, hogy m és n nem relatív prímek, pedig a feltétel az volt.)

Azaz az összes esetet megvizsgálva arra jutottunk, hogy egyedül az

$$a=2,\quad b=3,\quad p=2$$

számhármas elégíti ki az egyenletet.

4.3. Ne légy racionális!

Bebocsátást nyertetek! De csak akkor maradhattok, ha helyesen válaszoltok erre a kérdésre: létezik-e olyan négyzet, amelynek az oldalhossza racionális, és a területét valamint az oldalhosszát megszorozva egy-egy kettőnél nagyobb prímmel az összeg egy harmadik kettőnél nagyobb prím lesz? Azaz a matematika nyelvén: legyenek p, q, r 2-nél nagyobb prímek. El kell dönteni, hogy a

$$px^2 + qx - r = 0$$

egyenletnek lehet-e racionális gyöke! (Gerőcs–Orosz–Paróczay–Szászné Simon 2006:59)

Segítő kérdéseken keresztül a feladat megoldása:

Akkor létezik racionális gyöke, ha a diszkrimináns négyzetszám. Jelen esetben akkor lenne racionális gyök, ha az alábbi egyenletnek lenne p, q, r prím megoldása:

$$q^2 + 4pr = n^2$$

$$4pr = n^2 - q^2 = (n - q)(n + q)$$

Ekkor mivel a q páratlan prím négyzetéhez adjuk hozzá a $4pr$ páros számot, így az összegük páratlan lesz, ezért n^2-nek is páratlannak kell lennie, azaz n is páratlan. Legyen $n = 2k + 1$, $q = 2l + 1$.

Ekkor:

$$4pr = (2k + 1 - 2l - 1)(2k + 1 + 2l + 1) = 4(k - l)(k + l + 1)$$

$$\Downarrow$$

$$pr = (k - l)(k + l + 1)$$

$(k - l)$ és $(k + l + 1)$ különböző paritásúak, hiszen a különbségük $2l + 1$. Viszont a pr szorzatot csak páratlan szorzótényezőkre tudom felbontani. Azaz ennek az egyenletnek nincs megoldása, az eredetinek pedig nincsen racionális gyöke.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

Erdős és a pénzjutalmak

,,...10 éves koromban édesapám elmondta annak bizonyítását, hogy végtelen sok prímszám van, és hogy a prímszámok között tetszőlegesen nagy hézagok vannak, így barátságom a prímszámokkal korán kezdődött.” — írja Erdős Pál (Erdős 1997), a 20. század egyik legjelentősebb magyar matematikusa. A ,,hajléktalan matematikusként” is emlegetett, világjáró tudós rengeteg problémát, sejtést fogalmazott meg, vagy hozott be a köztudatba, és az általa vélt nehézség alapján bizonyos összegeket ígért a megoldóknak, pár dollártól akár több ezer dollárig. Például Szemerédi Endre, a 2012-ben Abel-díjjal kitüntetett magyar matematikus, 1972-ben egy fél évszázada

megoldatlan kérdést zárt le. Belátta, hogy — ,,konyhanyelven szólva" — kellően sok természetes számból álló halmazban biztosan lesz tetszőlegesen hosszú számtani sorozat. 1000 dollár ütötte a markát, tudomásunk szerint ez volt a legnagyobb összeg, amelyet Erdős kifizetett egy megoldásért. Szemerédi tételét később Terence Tao és Ben Green gondolta tovább, és belátták, hogy van tetszőlegesen hosszú, prímekből álló számtani sorozat.

Erdős természetesen maga is rendkívüli eredményeket ért el, például elsőéves egyetemistaként elemi bizonyítást adott Csebisev tételére, amely szerint minden n-re van prímszám n és $2n$ között.

Persze rengeteg nyitott kérdéssel küzdenek még ma is a számelmélet szakértői: például létezik-e végtelen sok ikerprím, azaz két olyan prím, melyek különbsége kettő. De ahogy Erdős a Mersenne-prímekről fogalmazott: ,,ez talán a legnehezebb (bár nem a legsürgősebb) megoldatlan probléma, mellyel az emberiség szembenéz." (Erdős 1993)

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

4.4. A szórakozott öregurak

Helyesen feleltetek, így a városban maradhattatok. A főtérre érve arra lettetek figyelmesek, hogy mindenki fejét fogva szaladgált, hatalmas csomagokkal igyekezett elhagyni a lakóhelyét. Három kissé szórakozott öregúr viszont nyugodtan üldögélt. Odamentetek hozzájuk, hogy a riadalom okáról érdeklődjetek. Ők viszont csak egy feladat árán voltak hajlandóak beavatni a rejtély részleteibe: azt állítják, hogy a szőnyeg, amin ülnek, a számegyenes, egyenlő távolságra vannak egymástól, és mindhárman egy-egy prím reciprokai. Meg kellett győzni őket arról, hogy tévednek! (Gerőcs – Orosz – Paróczay – Szászné Simon 2006:58)

Segítő kérdéseken keresztül a feladat megoldása:

Mivel reciprokaik egy számtani sorozat egymást követő tagjai, így az első és az utolsó tag számtani közepe éppen a második tag lesz, azaz ha $p < q < r$, akkor

$$\frac{\frac{1}{p} + \frac{1}{r}}{2} = \frac{1}{q}$$

Átrendezés után:

$$q = \frac{2pr}{r+p} = \frac{2p(r+p) - 2p^2}{r+p} = 2p - \frac{2p^2}{r+p}$$

Mivel p prím, így $2p^2$ csak 1-gyel, 2-vel, p-vel, $2p$-vel, p^2-tel és $2p^2$-tel osztható. Ezek közül, mivel p és r prímek, összegük csak az utóbbi három értéket veheti fel. Ám mi történne ekkor? Mivel az összeg is osztható p-vel, és p is osztható p-vel, így r is osztható lesz p-vel. Mivel prím, így ekkor csak p lehetne. Ám a feladat kikötése szerint különböző prímeket keresünk, tehát nincs megoldása a feladatnak.

4.5. A prímallergia

Az öregurak elfogadták érveléseteket. Így elmesélték, hogy egy különös betegség ütötte fel a fejét a városban: kitört a prímallergia. Nagyon gyorsan mindenkinek szüksége volt egy kódszámra, ám ez csak összetett szám lehetett, és a sorrendet tartani kellett: azaz egymást követő számok jöhettek csak szóba. Mit tettetek, ha tudjuk, hogy 2500-an élnek a városban? És ha többen?

Segítő kérdéseken keresztül a feladat megoldása:

Elkezdhetjük sorolni, ám egy idő után el fogunk akadni. Például: 9, 10 utána ott a 11. Vagy 32, 33, 34, 35, 36 után ott a 37. Valahogy mindig beleütközünk egy prímbe. De mivel egymást követő számokról beszélünk, így adódik a felírás:

$$a, a+1, a+2, ..., a+2499$$

Egy összegről mikor tudjuk biztosan, hogy egy szám az osztója? Ha mindkét tagját osztja. Tehát például $a+3$ akkor lesz osztható 3-mal, ha az a is osztható 3-mal. És ugyanennek az a-nak oszthatónak kell lennie 4-gyel is az $a+4$ miatt. Ezt a gondolatmenetet folytatva 2499-cel is oszthatónak kell lennie. Viszont lesz egy kis baj: az $a+1$ ezek közül egyikkel sem lesz osztható. Így $a+2$-vel kell kezdenünk, ennek következtében $a+2501$-gyel befejeznünk.

Tehát szükségünk van egy olyan a-ra, amely osztható 2-vel, 3-mal, 4-gyel, ... , 2501-gyel. Hogyan tudnánk legegyszerűbben ilyen a-t ,,csinálni"? Szorozzuk össze ezeket a számokat! Így $2501!$ lesz az eredmény. Tehát az egymást követő összetett számok:

$$2501!+2, 2501!+3, 2501!+4, 2501!+5, ..., 2501!+2501$$

Ha pedig k db embernek van szüksége erre, akkor:

$$(k+1)!+2, ..., (k+1)!+k+1.$$

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

Pénzünk biztonsága

A későbbiekben látni fogjuk, hogy milyen nagy kincs egy hatalmas szám prímtényezős felbontásának ismerete. Többek között a bankok is azt használják ki adataik védelmére, hogy egy több százjegyű számot szinte lehetetlen prímtényezőkre bontani. Erről beszélt Lovász László, Wolf-díjas matematikus Staar Gyula kérdésére válaszolva:

,,*Említetted, hogy a világ csaknem összes számítógépes rendszerének, így a bankoknak a biztonsága is, a prímszámokon, a nyilvános kulcsú titkosításon alapul. Létezhet gyors algoritmus ennek a rendszernek a feltörésére?*

- Ha van fontos kérdése a matematikának, akkor ez az! Vajon egy ezerjegyű számot fel lehet-e bontani hatékonyan prímtényezőire? Ha valaki megbirkózik ezzel a feladattal, akkor kérdésessé teszi a számítógépek biztonságát, aminek beláthatatlan következményei lennének. Összeomlana a rendszer. Nem hiszem, hogy ez egyik napról a másikra bekövetkezhet. A számítógépek biztonsága azon múlik, hogy van egy jókora rés azon két feladat bonyolultsága között, hogy mennyi idő alatt ellenőrizhetjük egy számról, hogy prímszám-e, illetve ha már tudjuk róla, hogy összetett szám, akkor annak mik a prímtényezői. Ez utóbbi kérdés megválaszolása sokkal nehezebb. Amíg ez a hézag létezik, addig beállíthatjuk úgy a rendszert, hogy az egyik feladat megoldható, a másik már nem. Alapvető fontosságú lenne valamilyen bizonyítást adni arra, létezhet-e olyan algoritmus, mely reális időn belül megoldja a nagy összetett számok prímtényezőre bontásának problémáját. Ettől azonban még messze vagyunk. Nem hiszek abban, hogy hirtelen olyan algoritmust találnak, ami képes feltörni a mai rendszert. Sokkal valószínűbb, hogy valaki publikál egy algoritmust, majd azt kemény munkával évekig javítgatják, végül eljutnak olyan szintre, hogy áttörjék vele a falat." (Staar 2006)

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

A város ünnepel titeket! Nem kell elmenekülni, nyugodtan élhetnek tovább. Így már tényleg nincs más feladatotok, mint a kincsvadászatra koncentrálni.

5. A titkos kulcs a győzelemhez

Most, hogy tudtátok a kincs pontos koordinátáit, és a városban leselkedő veszélyeket is hárítottátok, meg kellett keresnetek a kincset. Viszont egy nagy akadály még legyőzésre várt. A kincset csak akkor kaphattátok meg, ha a titkos jelszó birtokában vagytok. Ám ezt csak Rejtelmes Sehollakó Anonymus *ismerte, egy rendkívül titokzatos figura. Nem tudni, ki ő, hol lakik, honnan jött. Nem találkozhattatok vele, csak nyilvánosan tudtatok üzenni neki. Ez alapján tudta titkosítani a jelszót, amit utána ő is nyilvánosan közölhetett. De olyan módszerre volt szükség, amivel ezek után csak ti tudtátok megfejteni a nyilvánosan közölt információk alapján titkosított, nyilvánosan közölt kódot. Ez elég lehetetlennek tűnik, igaz? Ne aggódjatok, egy kedves hölgy, Izabella, segített nektek. Viszont ahhoz, hogy eljussatok hozzá, illetve az eljárást megismerjétek, pár próbatételt ki kellett állnotok:*

10. próbatétel: A titkos táblázat
11. próbatétel: Üzenj minden rubrikával!
12. próbatétel: Jani javaslata
13. próbatétel: A titkos x
14. próbatétel: Kincstári számvetés
15. próbatétel: Kulcskérdés
16. próbatétel: A Nagy Háromezerkarú Osztófosztó
17. próbatétel: A titkos kitevő
18. próbatétel: Lakat a számon
19. próbatétel: A kíváncsi futár
20. próbatétel: A hihetetlen titkosító eljárás

Most jött a legnehezebb része az utazásnak, sok sikert hozzá!

5.1. A titkos táblázat

A csapat egy része ügyesen megszerezte az Izabellához vezető út térképét. Titkosan közölni szerették volna veletek egy helyszínt, ahol találkozhattok. Ehhez titokban megkaptátok tőlük az alábbi táblázatot:

0	0	1	0	0
0	1	0	0	0
0	0	0	1	0
0	0	0	0	1
1	0	0	0	0

Majd feltették a Facebook-oldalukra ezt:

E	R	N	A	M
O	Y	I	M	F
P	R	T	I	E
O	G	K	N	P
U	A	C	I	U

Hol volt a találkozó? (T. Dénes 2004: 91–99)

Segítő kérdéseken keresztül a feladat megoldása:

5.1.1. Vajon milyen összefüggés lehet a két táblázat között?

Láthatjuk, hogy a méretük megegyezik, így elképzelhető, hogy egymásra illeszthetők, esetleg egy-egy betű megfeleltethető az első táblázat számaival.

5.1.2. Milyen megfeleltetést tudtok elképzelni?

Már többször láthattuk, hogy az 1-es valaminek a létét jelenti, valamit veszünk, számolunk, kiválasztunk, míg a 0 éppen azt jelenti, hogy azt a dolgot nem vesszük, nem választjuk.

5.1.3. Ennek fényében mit rejthet az üzenet?

Az 1-esek helyén lévő betűket összeolvasva: a NYIPU a találkozó helye. Ezt még dekódolni kell: minek lehet a rövidítése? Nyugati pályaudvar.

5.1.4. Mik lehetnek az ilyen titkosítás előnyei?

Például egy újságcikket is felhasználhatunk szövegként, ha valamilyen oknál fogva nem tudunk hosszabb üzenetet eljuttatni.

5.1.5. Mik lehetnek az ilyen titkosítás korlátai?

Például túl rövid üzenetet lehet csak közölni.

Mivel társaink több információt akartak titkosan megosztani velünk, így egy kicsit csiszoltak módszerükön:

5.2. Üzenj minden rubrikával!

Most az alábbi táblázatot juttatták el hozzátok:

4	1	2	5	3
2	5	3	4	1
3	4	1	2	5
1	2	5	3	4
5	3	4	1	2

Majd ezt a táblázatot tették közre:

N	H	A	H	A
N	E	T	Z	A
I	T	T	Y	T
O	G	F	P	A
O	E	R	R	G

Mit üzenhettek? (T. Dénes 2004: 91–99)

Segítő kérdéseken keresztül a feladat megoldása:

5.2.1. Vegyük egy kicsit szemügyre az első táblázatot! Hogy helyezkednek el benne a számok?

Észrevehetjük, hogy minden sorban és minden oszlopban egy 1-es, egy 2-es, egy 3-as, egy 4-es és egy 5-ös van. Azaz, ha az 1-eseket leszámítva minden szám helyére 0-t írunk, akkor az előző feladatban látottak alapján azt olvashatjuk ki, hogy: HATOR.

5.2.2. De ezt még nem tudjuk értelmezni. Mi célt szolgálhat a többi szám?

Ha velük is úgy teszünk, mint az 1-essel, akkor kapunk egy táblát csupa 2-essel és 0-val és így tovább. Ezen táblákat sorra kiolvasva ezt a betűsort nyerjük:

$$HATORANYUGATIPENZTARHETFO$$

Azaz: hétfőn hat órakor a Nyugati pályaudvar pénztárjánál lesz a titkos találkozó. Láthatjuk, hogy így jelentősen hosszabb üzenetet tudunk ugyanannyi betűvel és számmal közölni.

5.2.3. De mi lehet ennek a módszernek az egyik veszélye?

Mivel az üzenet betűit nem, csak a betűk sorrendjét változtattuk meg, így ügyes próbálgatással megfejthetik.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

Tudtad-e? Jules Verne és a titkosírás

Jules Verne, vagy ahogy itthon ismerhetitek, Verne Gyula, több híres művében jelenik meg a titkosírás a történet fontos mozgatórugójaként. Az *Utazás a Föld középpontja felé* című regényében a kissé bogaras hamburgi geológusprofesszor unokaöccsével karöltve egy titkosírással írt középkori dokumentumot fejtenek meg, például ilyen gondolatmenetek segítségével: ,,- Vizsgáljuk meg jól — vette újra kezébe azt a szöveget, amit én írtam le. — Ez a 132 betű látszólag rendetlenül követi egymást. Vannak szavak, melyekben csak mássalhangzók állnak, mint az elsőben: »mm.rnlls«, másokban éppen ellenkezőleg, túl sok a magánhangzó, mint például a második oszlop

második szavában: »unteief«vagy az utolsó előttiben: »oseibo«. Ezt az elrendezést biztosan nem találomra csinálták, hanem egy matematikai rendszer szerint állították sorba a betűket. Biztosra veszem, hogy eredetileg szabályosan leírták a mondatot, aztán valamilyen rendszer szerint megkeverték. Ezt a rendszert kell felfedezni. Aki megszerzi a titkosírás kulcsát, az folyékonyan olvashatja a szöveget. De mi ez a kulcs? Axel, tudod a kulcsát?" (Verne 1998) A regényben az üzenet megfejtése után tudják meg, hogy hol indulhatnak le a Föld középpontja felé.

A *Sándor Mátyás* című, Verne elképzelt magyar szabadságharcosáról szóló regényében is titkosírással találják szembe magukat a szereplők. Carlo Zirone és Sárkány szövetkeztek Sándor Mátyás ellen, aki részt vett a magyarok által szervezett összeesküvésben. Az összeesküvők egy postagalambbal üzentek egymásnak, ám Sárkányék kezébe került a titkos szöveg: három darab 6x6-os négyzetből állt a táblázat, s benne minden rubrikában egy betű szerepelt. A megfejtéshez egy bizonyos rácsot kellett használni, amely segítségével erre a megfejtésre jutottak: ,,MINDEN KÉSZEN ÁLL. AZ ÖN TRIESZTBŐL ÉRKEZŐ LEGELSŐ JELÉRE AZONNAL NAGY TÖMEGEK KELNEK FEL MAGYARORSZÁG FÜGGETLENSÉGÉÉRT. XRZAH".(Verne 1980)

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

5.3. Jani Javaslata

Szerencsésen megfejtettétek a többiek üzenetét, így tudtátok, hogy hatkor a Nyugatinál kell lennetek. Ezalatt a csapat másik fele is tanakodott, valami olyan módszert szerettek volna kitalálni, amihez nem kell táblázat. Jani azt javasolta, hogy minden magánhangzót cseréljenek ki egy csillagra, minden mássalhangzót egy x-re. Hogyan beszélnétek le Janit erről az ötletről?

Segítő kérdéseken keresztül a feladat megoldása:

5.3.1. Azt gondoljuk végig, hogy az üzenet küldője, vagy fogadója kerül nehéz helyzetbe?

Könnyen láthatjuk, hogy így kódolni pofonegyszerű. Például a ,,holnap ott várlak" így nézne ki: ,,$x * xx * x * xxx * xx * x$". Viszont, ha egy ilyen üzenetet kapunk, akkor törhetjük a fejünk napestig. Például lehet az üzenet ,,tegnap ezt vettem", vagy végtelen sok más. Szinte lehetetlen megfejteni, pedig tudjuk a kulcsot.

Mi lehet a probléma Jani módszerével? Amikor kódoljuk az üzenetet, akkor tudjuk, hogy mit mivel feleltessünk meg, viszont visszafelé ez már nem megy. Azaz nem kölcsönösen egyértelmű. Ez azért gond, mert egy olyan megfeleltetésre van szükségünk, aminek a ,,fordítottját", azaz inverzét végrehajtva a kódolt üzeneten, visszakapnánk az eredetit.

5.4. A titkos x

A többiek tanultak Jani ötletéből, így valami újat fundáltak ki, és ezzel üzentek még a találkozó előtt. Titkos úton eljuttatták hozzátok azt, hogy $x + 2$, majd ezt a betűsort közölték az iskolaújságban:

„ÍÖAABUÖLYFTQLYBCSCUÖU". Mi lehetett a jelentése?

Segítő kérdéseken keresztül a feladat megoldása:

5.4.1. Mit jelenthet az $x + 2$ titkos üzenet?

Mivel Jani tanult a hibás gondolatmenetéből, így bizonyára elmondta nekik, hogy ügyeljenek arra, hogy minden betűt különböző szimbólumokkal feleltessenek meg. Ezen felül azt is láthatjuk, hogy a magyar ábécét használták, azaz a magyar ábécé betűit a magyar ábécé betűivel feleltették meg. Már csak a megfeleltetés logikájára kell rájönnünk.

A betűk kölcsönösen egyértelmű megfeleltetése előhívja bennünk a függvény fogalmát. Láthatjuk, hogy jelen esetben az értelmezési tartományunk és az értékkészletünk is a magyar ábécé. Tehát az $x + 2$ üzenetet úgy is értelmezhetjük, hogy

$f(\text{betű}) = \text{betű} + 2$.

De ezt hogy értelmezzük? Mivel előzetesen nem beszéltünk meg egy különleges megfeleltetést, így a legegyszerűbbre kell gondolnunk: a betűt a sorszáma szimbolizálja, így az $x+2$ utasítás alapján a sorszámához kell kettőt hozzáadni. Ez alapján az A-hoz a C-t, a B-hez a Cs-t, ..., a Z-hez az A-t, a Zs-hez az Á-t rendeli.

5.4.2. Egy dolog még tisztázásra vár: ez a mi „dekódolós" szabályunk, vagy a saját szabályukat küldték el?

Ezt csak próbával tudjuk eldönteni. Először az első eshetőséggel számoljunk: tehát azzal, hogy a mi szabályunkat küldték el. Ekkor így néz ki az üzenet, alatta a dekódolt jelentéssel:

Í	Ö	A	A	B	U	Ö	LY	F	T	Q	LY	B	CS	C	U	Ö	U
K	P	B	B	CS	Ü	P	N	GY	U	S	N	CS	DZ	D	Ü	P	Ü

Ez úgy tűnik nem vezet eredményre. Így feltételezhetjük, hogy a saját képzési szabályukat küldték el. Tehát, ha ők minden betűt a kettővel utánakövetkezővel cseréltek ki, akkor mi lesz a mi teendőnk? Azaz mi az $f(x) = x + 2$ függvény inverze?

Kis gondolkodás után, vagy az $y = x+2$ alapján az $x = y-2$ egyenlettel dolgozva könnyen adódik, hogy az $x - 2$ lesz a mi függvényünk.

Ez alapján a megfeleltetés így néz majd ki:

Í	Ö	A	A	B	U	Ö	LY	F	T	Q	LY	B	CS	C	U	Ö	U
H	O	Z	Z	A	T	O	K	E	S	Ő	K	A	B	Á	T	O	T

Összeolvasva máris értelmet nyer az üzenet: ,,hozzatok esőkabátot".

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

Tudtad-e? Az első hacker

A titkosírás igen elterjedt volt a 9-10. századi arab közigazgatás világában, rengeteg dokumentumot titkosítottak. A legegyszerűbb módszerek egyikével, a monoalfabetikus behelyettesítéssel rejtették el információikat. Ez annyit tesz, hogy minden betűt kicseréltek egy másik betűvel, jellel. Az eljárás természetesen a ,,hackerek" figyelmét is felkeltette. Mai tudásunk szerint az arabok jöttek rá először a titok nyitjára. Észrevették, hogy bizonyos betűk gyakrabban, bizonyosak kevésbé gyakran fordulnak elő egy-egy hosszabb szövegben. Először Jákúb ibn Iszhák al-Kindi vetette papírra módszerét a 9. században: ,,Ha tudjuk, milyen nyelven íródott a kódolt üzenet, akkor megfejtésének egyik módja az, hogy veszünk egy ugyanolyan nyelven írt nyílt szöveget, amely elég hosszú ahhoz, hogy legalább egy lapot megtöltsön, és megszámláljuk, melyik betű hányszor fordul elő benne. (...) Ezután vesszük a kódszöveget, s annak szimbólumait is megszámláljuk. Megkeressük a legsűrűbben előfordulót, s azt behelyettesítjük a nyílt szöveg leggyakoribb betűjével..." (Singh 2001: 28) — tehát Jákúb lényegében a gyakoriságelemzést fogalmazta meg. Ez a fegyver szinte mindig bevethető volt a helyettesítéssel kódolt szövegek esetén.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

5.5. Kincstári számvetés

Még szerencse, hogy megfejtettétek az előző üzenetet, ugyanis amíg a pályaudvarhoz közeledtetek, elkezdett zuhogni az eső. Úgy tűnik, a többiek a jövőbe láttak. Pontban hatkor találkoztatok is velük a pénztárnál. Át is adták a térképet, és sejtelmesen mosolyogtak.

A térkép egy titkos alagutat jelzett, pár méterre a pénztáraktól. Gyorsan a jelölt helyre szaladtatok. Itt, egy eldugott zugban, megtaláltátok a lejárót, és leszaladtatok. Egy vonat várt benneteket. A kalauz idegesen feltessékelt titeket a különös szerelvényre, majd elindultatok. Még alig ocsúdtatok fel az izgalommal teli ijedtségből, megjelent a kalauz. Megköszörülte a torkát, és így szólt: ,,Csak akkor utazhatnak a vonaton, ha elmondják, hogy összesen mekkora a vagyonuk." — értetlenül néztetek egymásra. A legtöbb ember nem szívesen mondanák el, hogy pontosan mennyi pénzük van. Hogyan tudhattátok meg ezt az összeget, ha senki sem akarta nyilvánosságra hozni, hogy mekkora a vagyona? (Csirmaz 2006)

Segítő kérdéseken keresztül a feladat megoldása:

5.5.1. Hogyan álljunk neki?

Mivel összegről van szó, így bizonyos értékeket biztosan össze kell adni. Mi az, ami egy összegen nem változtat? Ha egy számot és az ellentetjét is hozzáadjuk. Azaz jelen esetben az elején indíthatunk egy tetszőleges számmal, ha a végén ki is vonjuk. De ez miért segít? Ha én kezdem az összegzést, akkor a saját vagyonomat nem akarom elmondani. Viszont, ha egy általam kreált titkos számhoz adom hozzá, akkor a többiek nem tudják meg vagyonom nagyságát. De innen hogyan léphetnénk tovább? Ha ezt nyilvánosságra hozom, akkor a többiek ugyanott tartanak, ahol a legelején. Viszont, ha csak egy embernek mutatom meg, akkor ő nyugodt szívvel hozzáadhatja a sajátját, senki sem tudja, hogy mi volt az eredeti szám (kivéve engem, így ezt az összeget én nyilván nem láthatom). Az így kapott értéket hasonlóan továbbadhatja egy embernek, aki ehhez adhatja tovább a saját vagyonát és így tovább.

5.5.2. Hogyan tudjuk meg az összeget?

Ha az utolsó ember is hozzáadta saját értékét, akkor még ki kell vonni az így kapott számból azt, amit én az elején hozzáadtam. (Természetesen kivonás előtt csak nekem adja át, hiszen az engem követő illető, ha látná kivonás előtt is az értéket, akkor tudna következtetni a vagyonomra). Tehát az eddigi ,,egy az egynek" átadással megkapom azt az összeget, amely a kezdőérték és mindannyiunk vagyonának összege. Ebből kivonva a kezdőértéket megkapjuk a szükséges számot úgy, hogy senki sem szerzett tudomást a többiek vagyonának nagyságáról.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

Kossuth Lajos azt üzente

Jules Verne *Sándor Mátyás* című regényében 1848-as titkos összeesküvésről olvashatunk. A valóságban is akadtak olyanok, akik a forradalom idején rejtett utakon igyekeztek sikerre jutni. Ilyen volt Makk József. Részt vett a Klapka György elleni összeesküvésben, ugyanis társaival együtt azt gondolta, hogy a komáromi várvédők vezetője hazaárulást követ el azzal, hogy hajlandóságot mutat a Haynauval való megállapodásra. Helyette Makkot (ekkor még Mackot) akarták fővezérnek kinevezni, s az osztrákoknak nem engedve Komáromot és Csallóközt szabad köztársasággá kikiáltani (Jókai 2001). A sikertelen próbálkozás után börtön és bujdosás volt Makk osztályrésze. 1851-ben Kossuth Lajoshoz is eljutott Törökországba, akitől írásbeli felhatalmazást kapott egy új forradalmi mozgalom megszervezésére. Ezt követően titkos levélváltásba kezdtek: ,,A bukaresti Kriterion Könyvkiadó közkedvelt Téka-sorozatában megjelent *Székely vértanúk 1854* című kötet az összeesküvéssel kapcsolatos leveleket, visszaemlékezéseket tartalmazza. Érdekes logikai játékot kínál a Kossuthnak Makkhoz írt 1851. szeptember 8-i levele. A magyar nyelvű levélben 12 szót titkosírással írtak, a betűk helyett számok szerepelnek. Makk gyakran hangoztatta a bibliai tanácsot: legyetek óvatosak, mint a kígyók. A kötet közli a titkosírással írt és a dekódolt szöveget is." (Jéki 2004) Szerencsétlenségükre a dekódolás az osztrák hatóságoknak sem okozott gondot, ugyanis a levelek mellett a rejtjelezés kulcsa is a

kezükre jutott. Így 1851 őszén csírájában fojtották el a mozgalmat, több résztvevőt később kivégeztek. Makk Józsefnek sikerült emigrálnia, később egy amerikai katonai akadémián dolgozott matematikatanárként.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

5.6. Kulcskérdés

Szerencsésen rendeztétek az ügyet a kalauzzal. Pár perccel később, valahol Budapest alatt megállt a vonat. Elindultatok a kijárat felé, amikor legnagyobb meglepetésetekre a vonatban egy majd' tíz méter magas ajtó fogadott benneteket. Az ajtó barázdált fatestén méterenként tíz zár rozsdásodott. Kalauzunk a következő útmutatással látott el titeket: ,,Tíz kulcsnál többet használjatok, annyit, amennyiből, ha hármasával mérjük, egy marad ki, ha ötösével, akkor három, ha pedig tizenegy egy kupac, akkor hét. A megfelelő számú kulcsot az alsó záraktól kezdve helyezzétek a lyukakba! De csak egyszer próbálkozhattok!" Hogyan lehetett megoldani a talányt?

5.6.1. Számoljuk le!

Hirtelen Hedvig így kiáltott: ,,Összesen száz zár van, az nem olyan sok. Valahogy okosan próbálkozzunk!" Lassúvíz Lajos így csitította: ,,Igaz, most nincs olyan sok lehetőség a tizenegyes miatt, de érdemes rendesen átgondolni, hiszen kerülhetünk még olyan akadály elé, ahol a találgatás nem segít." Hedvig szeme villámokat szórt. Biztos volt igazában, így gyorsan nekiállt megtalálni a megoldást:

,,Ha hármasával számolva egy marad ki, az a matematika nyelvén annyit tesz, hogy hárommal osztva egy maradékot ad. Ilyen számokból elég sok van még száz alatt is. A második információ okán a keresett szám öttel való osztási maradéka három, még ez is sok próbálkozás lenne. Viszont, ha tizenegyesével számoljuk le a kulcsokat, akkor hét marad ki. Ilyen értékből már nincs olyan sok száz alatt." — örvendezett Hedvig. Lajos is látta, hogy barátja jó nyomon jár, így dacolva büszkeségével gyorsan sorolta: ,,Igazad van, ilyen a 18, a 29, a 40, az 51, a 62, a 73, a 84 és a 95." Érezték, hogy közel a megoldás. Már csak a hármas és az ötös maradékokat kellett megvizsgálni. Hamar látták, hogy hárommal osztva egy maradékot csak a 40 és a 73 ad. Pár pillanat múlva Hedvig és Lajos egyszerre kiáltották: ,,Gyorsan számoljatok 73 kulcsot!", hiszen a 40 osztható öttel, a 73 viszont három maradékot ad.

A csapat többi része sorra dugdosta be a kulcsokat a zárakba, egymásra állva óriási tornyot képezve már a legfelső lyukaknál jártak. Az emberpiramis csúcsára Hedviget és Lajost juttatták, hogy az utolsó kulcsot a két megoldó dughassa be. A 73. rozsdás zár nehezen, de benyelte ,,eledelét", a hatalmas kapu pedig kitárult a kalandorok előtt. Hedvig a magasban Lajosra kacsintott, és így szólt: ,,A nehezebb feladatnál, ígérem, rád hallgatok. Akkor majd alaposabban átgondoljuk." Lajos

elégedetten fogadta a lány szavait. Nem is tudhatták, hogy nem is olyan sokára milyen nagy szükség lesz Lajosra.

5.7. A Nagy Háromezerkarú Osztófosztó

Eszeteknek köszönhetően lejutottatok a vonatról. A föld alatt voltatok, de egy létrán szerencsésen felmászhattatok. Kisvártatva egy furcsa lénnyel találkoztatok. Ő volt a Nagy Háromezerkarú Osztófosztó. Az ő tudománya abból állt, hogy minden olyan számot, amit le tudott osztani a 3000 valamely 1-től különböző osztójával, bekebelezett, és minél többet evett, annál vérszomjasabb lett. A szörnyetegen akkor juthattatok át, ha az előttetek lévő, 1-től 3000-ig megszámozott sütikből a lehető legtöbbet átvittétek a szörnyön. De ha akár csak egyet is megevett, akkor vége volt mindennek. Hány sütit vihettetek magatokkal?

Segítő kérdéseken keresztül a feladat megoldása:

5.7.1. Mi is a feladat?

A 3000 összes, 1-nél nagyobb osztója lesz a szörny fegyvere. Azaz a 2, 3, 4, 5, 6, 8, ... 1500, 3000. Ha az általunk kiválasztott süti sorszáma ezek közül bármelyikkel osztható, akkor vesztettünk. Tehát a kiválasztott sütik sorszámának és a 3000-nek nem lehet 1-nél nagyobb közös osztója, relatív prímnek kell lenniük. ,,Gyorsan számoljuk végig, hogy ez hány darab!" — kiáltott Hedvig. ,,Gyorsan?!" - Értetlenkedett Lajos. — ,,Ezt mindennek nevezném, csak gyorsnak nem. És túl okosnak sem. Kell, hogy legyen ebben valami szabályosság." Kis gondolkodás után Lajos azt tanácsolta, hogy előbb vizsgáljanak meg kisebb számokat, hátha rájönnek a logikájára.

Így megnézték a 10-et. Relatív prím a 10-hez: 1, 3, 7, 9. Nem relatív prím: 2, 4, 5, 6, 8, 10. Láthatjuk, hogy az összes 2-vel vagy 5-tel osztható szám szerepel a felsorolásban.

Nézzük meg a 15-öt! Relatív prím a 15-höz: 1, 2, 4, 7, 8, 11, 13, 14. Nem relatív prím: 3, 5, 6, 9, 10, 15. Itt azt vesszük észre, hogy a második listán az összes 3-mal vagy 5-tel osztható szám szerepel.

Mindkét példánál láthattuk, hogy a relatív prímekre az igaz, hogy a megadott szám egyik osztójával sem oszthatók (például az összes 10-et, 15-öt nem osztó prím szerepelt a felsorolásban), a nem relatív prímek pedig az adott szám egyik vagy másik (itt a vagy megengedő vagy, tehát a mindkettővel való oszthatóságot is beleértjük) osztójával osztható. ,,Akkor talán érdemes lenne a második lista nagyságát kiszámolni, és azt kivonni az eredeti számból." — mondta lelkesen Lajos. A 10-nél és a 15-nél könnyű dolguk volt.

5.7.2. De hogyan okoskodjanak egy nagyobb számnál?

Próbáljuk ki 100-zal! Ehhez kellene a 100 összes 1-nél nagyobb osztója. Ezt még fel tudjuk sorolni: 2, 4, 5, 10, 20, 25, 50, 100. Ennyi szám osztható 100-ig:

2-vel	50
4-gyel	25
5-tel	20
10-zel	10
20-szal	5
25-tel	4
50-nel	2
100-zal	1

Viszont ezeket nem adhatjuk csak úgy össze, hiszen a 2-vel oszthatók között vannak 5-tel oszthatók is, a 4-gyel oszthatók mind oszthatók 2-vel és így tovább. Tehát valamilyen logika szerint le kellene számolnunk, hogy ez hány különböző számot jelent.

Vegyük az összes 2-vel oszthatót: 50 db, adjuk hozzá az összes 5-tel oszthatót: 20 db. Most hol tartunk? A 2-vel oszthatókkal együtt beleszámoltuk a 4-gyel oszthatókat, az 5-tel oszthatók miatt a 25-tel oszthatókat, a $2 \cdot 5 = 10$-zel (tehát a 20-szal, 50-nel, 100-zal) osztható számokat is leszámoltuk. Abban biztosak lehetünk, hogy maximum 70 nem relatív prím van, hiszen mindent beleszámoltunk. Viszont például a 10-et számoltuk a 2-esnél és számoltuk az 5-ösnél is. Minden 10-zel oszthatót kétszer számoltunk, tehát egyszer le kell vonni (és semmi mást nem számoltunk kétszer).

Tehát a 100-hoz nem relatív prímek száma: 50 + 20 - 10 = 60. Így a 100-hoz relatív prímek száma: 100 - 60 = 40.

5.7.3. És a prímtényezők?

„Érdemes lenne a prímtényezőket valahogy szerepeltetni a felírásban, hogy jobban lássuk a logikáját!” — ajánlotta Hedvig, aki belátta, hogy Lajos logikája fogja őket sikerre juttatni.

$$100 = 2^2 \cdot 5^2$$

2-vel osztható számok:	$\frac{100}{2} = 50$
5-tel osztható számok:	$\frac{100}{5} = 20$
10-zel osztható számok:	$\frac{100}{10} = 10$

100-hoz nem relatív prímek száma: $\frac{100}{2} + \frac{100}{5} - \frac{100}{10}$,

100-hoz relatív prímek száma: $100 - \frac{100}{2} - \frac{100}{5} + \frac{100}{10}$.

1000 esetén, mivel két különböző prímtényező szerepel a felbontásban, így hasonlóan kell eljárni: 1000 - 500 - 200 + 100 = 400 relatív prímet fogunk találni.

5.7.4. De mi a helyzet ha három különböző prímtényező szerepel?

$$3000 = 2^3 \cdot 3 \cdot 5^3$$

Ugyanúgy leszámoljuk, hogy hány szám osztható 3000-ig

2-vel osztható számok	$\frac{3000}{2} = 1500$
3-mal osztható számok	$\frac{3000}{3} = 1000$
5-tel osztható számok	$\frac{3000}{5} = 600$

Ez összesen 3100. Mit hányszor számoltunk? 2-szer számoltuk a $2 \cdot 3 = 6$-tal, $2 \cdot 5 = 10$-zel és a $3 \cdot 5 = 15$-tel osztható számokat. Mit számoltunk háromszor? A $2 \cdot 3 \cdot 5 = 30$-cal osztható számokat. Ha kivonjuk a 6-tal, 10-zel és 15-tel osztható számok mennyiségét, akkor mindhárom esetben levontuk a 30-cal oszthatókét, így azt egyszer sem számoltuk, tehát még egyszer hozzá kell adni.

A 3000-hez nem relatív prímek száma: $\frac{3000}{2} + \frac{3000}{3} + \frac{3000}{5} - \frac{3000}{6} - \frac{3000}{10} - \frac{3000}{15} + \frac{3000}{30}$ = 1500 + 1000 + 600 - 500 - 300 - 200 + 100 = 2200, tehát a 3000-hez relatív prímek száma: 3000 - 2200 = 800.

5.7.5. ,,De jó lenne általánosítani!"

— sóhajtott Lajos. ,,Próbáljuk meg" — biztatta Hedvig. Így nekiláttak. Legyen $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} ... \cdot p_{r-1}^{\alpha_{r-1}} \cdot p_r^{\alpha_r}$ a szám. Ki kell számolni, hogy hány n-hez relatív prím van n-ig. De érdemes most is a komplementert számolni, azaz, hogy hány szám van n-ig, amelynek van 1-nél nagyobb közös osztója n-nel.

Az előzőhöz hasonlóan először azt számoljuk ki, hogy a különböző prímtényezőkkel hány szám osztható n-ig

p_1 -gyel	$\frac{n}{p_1}$
p_2-vel	$\frac{n}{p_2}$
...	
p_r-rel	$\frac{n}{p_r}$

Ha ezeket összegezzük, akkor megint kétszer számoltuk a kétszeres szorzatokkal, azaz a $p_1 \cdot p_2$, $p_1 \cdot p_3$, ..., $p_{r-1} \cdot p_r$ szorzatokkal osztható számokat, így ezek számát le kellene vonni.

Általánosságban $p_i \cdot p_j$-vel $\frac{n}{p_i \cdot p_j}$ darab szám osztható n-ig.

Most meg kell vizsgálnunk, hogy a háromszoros szorzatokkal mi a helyzet! Például tekintsük a $p_1 \cdot p_2 \cdot p_3$ szorzatot. Az ezzel osztható számokat először vettük háromszor

p_1, p_2 és p_3 esetén. Majd levontuk $p_1 \cdot p_2$, $p_1 \cdot p_3$ és $p_2 \cdot p_3$ többszöröseinél, tehát jelenleg nullaszor vettük, így a hármas szorzatokat hozzá kell adni. Továbbgondolhatjuk, hogy a négy-, öt, ... , r-tényezős szorzatok esetén a szitaformulára jutunk, melynek helyessége a binomiális tétellel igazolható (erre most nem térünk ki):

az n-hez relatív prímek száma (ezt jelöljük $\varphi(n)$-nel, ugyanis a matematikában Euler-féle φ–függvénynek nevezik):

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \frac{n}{p_3} - ... - \frac{n}{p_r} + \frac{n}{p_1 \cdot p_2} + \frac{n}{p_1 \cdot p_3} + ...$$

$$... + \frac{n}{p_{r-1} \cdot p_r} - \frac{n}{p_1 \cdot p_2 \cdot p_3} - ... + (-1)^r \frac{n}{p_1 \cdot p_2 \cdot p_3 ... \cdot p_r}$$

5.7.6. Hogyan alakítsuk át?

,,Milyen fantasztikus lenne ezt szorzattá alakítani, akkor könnyebben alkalmazhatnánk bármilyen prímtényezős felbontásra!" — álmodozott Hedvig. Lajos a fejét vakarva így szólt: ,,Ha már eddig eljutottunk, ne torpanjunk meg. Hátha szükségünk lesz rá. Próbáljuk meg először valamilyen egyszerűbb esettel!"

Így nekiláttak a $k = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3}$ esetnek. Az előző számolások alapján

$$\varphi(k) = k - \tfrac{k}{p_1} - \tfrac{k}{p_2} - \tfrac{k}{p_3} + \tfrac{k}{p_1 \cdot p_2} + \tfrac{k}{p_1 \cdot p_3} + \tfrac{k}{p_2 \cdot p_3} - \tfrac{k}{p_1 \cdot p_2 \cdot p_3}.$$

Rögtön látható, hogy k kiemelhető. Utána szemfülesen észrevehetjük, hogy az $(1 - \frac{1}{p_1})$ is kiemelhető, méghozzá a következő módon:

$$\varphi(k) = k \cdot (1 - \frac{1}{p_1} - \frac{1}{p_2} - \frac{1}{p_3} + \frac{1}{p_1 \cdot p_2} + \frac{1}{p_1 \cdot p_3} + \frac{1}{p_2 \cdot p_3} - \frac{1}{p_1 \cdot p_2 \cdot p_3}) =$$

$$= k \cdot [(1 - \frac{1}{p_1}) - \frac{1}{p_2} \cdot (1 - \frac{1}{p_1}) - \frac{1}{p_3} \cdot (1 - \frac{1}{p_1}) + \frac{1}{p_2 \cdot p_3} \cdot (1 - \frac{1}{p_1})] =$$

$$= k \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2} - \frac{1}{p_3} + \frac{1}{p_2 \cdot p_3})$$

A második zárójelen belül az előzőhöz hasonlóan kiemelhető $1 - \frac{1}{p_2}$, így végül a következő alakot kapjuk:

$$\varphi(k) = k \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot (1 - \frac{1}{p_3})$$

Mi a helyzet, ha négy prímtényező szerepel a felbontásban? Legyen $m = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdot q_4^{\beta_4}$. Ekkor az előző alapján felírhatjuk a csak a q_1, q_2, q_3 tényezőket tartalmazó szorzatot, és hozzáadhatjuk a q_4-et is tartalmazó tagokat:

$$\varphi(m) = m \cdot (1 - \frac{1}{q_1}) \cdot (1 - \frac{1}{q_2}) \cdot (1 - \frac{1}{q_3}) - \frac{1}{q_4} + \frac{1}{q_1 \cdot q_4} + \frac{1}{q_2 \cdot q_4} + \frac{1}{q_3 \cdot q_4}$$

$$- \frac{1}{q_1 \cdot q_2 \cdot q_4} - \frac{1}{q_1 \cdot q_3 \cdot q_4} - \frac{1}{q_3 \cdot q_2 \cdot q_4} + \frac{1}{q_1 \cdot q_2 \cdot q_3 \cdot q_4}$$

Az előző kiemelések alapján (először $(1-\frac{1}{q_1})$-et, majd $(1-\frac{1}{q_2})$-t, végül $(1-\frac{1}{q_3})$-at kiemelve) erre juthatunk:

$$\varphi(m) = m \cdot [(1-\frac{1}{q_1}) \cdot (1-\frac{1}{q_2}) \cdot (1-\frac{1}{q_3}) - \frac{1}{q_4} \cdot (1-\frac{1}{q_1}) \cdot (1-\frac{1}{q_2}) \cdot (1-\frac{1}{q_3})] =$$

$$= m \cdot (1-\frac{1}{q_1}) \cdot (1-\frac{1}{q_2}) \cdot (1-\frac{1}{q_3}) \cdot (1-\frac{1}{q_4}).$$

Lassúvíz Lajos szeme csillogott az örömtől. ,,Tehát belátható, hogy amikor egy újabb tényezőt veszünk a szorzathoz, mondjuk q_i-t, akkor az addigi értéket szorozzuk meg $(1-\frac{1}{q_i})$-vel, tehát a fenti képletünk általánosítható!"

A fiatalok már nagyon közel jártak a könnyen használható képlethez. Gyorsan felírták az általános alakját:

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} ... \cdot p_{r-1}^{\alpha_{r-1}} \cdot p_r^{\alpha_r}$.

Ekkor:

$$\varphi(n) = n \cdot (1-\frac{1}{p_1}) \cdot (1-\frac{1}{p_2}) \cdot (1-\frac{1}{p_3}) \cdot ... \cdot (1-\frac{1}{p_r}).$$

,,Én nem szeretem a törteket, olyan nehézkes velük a számolás." — sóhajtott Hedvig. Kicsit nézegették a képletet, majd egyszerre kiáltottak: ,,Megvan!". Eszükbe jutott, hogy ha minden egyes tényezőt beszoroznának azon prím valamely hatványával, amely nevezőként szerepel, akkor nem kellene a törtekkel bíbelődniük. Majd látták, hogy a szorzat elején ott van az n, azaz adottak is ezek a szorzások, hiszen mindegyik p_i pontosan egyszer szerepel n-ben, és pontosan egyszer szerepel nevezőként. Így minden i-re (1-től r-ig) az $(1-\frac{1}{p_i})$-t $p_i^{\alpha_i}$-nel szorozták be. Végül ezt kapták:

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdot ... \cdot (p_r^{\alpha_r} - p_r^{\alpha_r-1}),$$

ahonnan már könnyedén kiszámolható bármely n-re az értéke.

Lajos azért a biztonság kedvéért ezt javasolta: ,,Gyorsan ellenőrizzük pár kicsi számra, ahol képlettel és leszámlálással is dolgozhatunk! Mondjuk 3-tól 10-ig:

n	3	4	5	6	7	8	9
$\varphi(n)$	2	2	4	2	6	4	6

Lajos megnyugodott, mert mindegyik esetben ugyanazt kapták eredményül a kétféle számolás után.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

Az első világháború kulcsa

A rádió feltalálása és a világméretű konfliktusok komoly hozzájárulást tettek a titkosírások kódolásának és dekódolásának fejlődéséhez. Ugyanis a hadi kommunikáció szinte kizárólagos tere a rádióhullámok voltak, ám az üzenetek könnyű lehallgathatósága miatt titkosításra volt szükség. Az első világháború folyamán bizonyos országok külön részlegeket hoztak létre, ahol az elkapott üzenetek megfejtése volt az egyedüli cél, ilyen volt Nagy-Britanniában a Room 40, azaz a 40-es szoba. Ken Follett, rendkívül népszerű brit író a 2012-ben megjelenő *Titánok bukása – Évszázad–trilógia* 1. részében éppen egy sorsdöntő üzenet megfejtéséről ír:

,,*Javasoljuk, hogy február elsején kezdődjön a korlátlan tengeralattjáró-hadviselés.*

Uramisten! – mondta Fitz. Előre féltek tőle, és most itt a megerősítés, ráadásul konkrét időponttal! Ez nagy siker a 40-es szobának!

Közben is törekszünk megőrizni Amerika semleges xxx. Ha nem sikerül, szövetséget ajánlunk (?Mexikónak?) a következő alapon: háború, aztán békekötés.

Szövetség Mexikóval? – kérdezte Fitz magától. – Ez erős. Az amerikaiak falra másznak tőle!

Excellenciád egyelőre tájékoztassa titokban az elnököt az Amerika elleni háborúról xxxx, és egyidejűleg tárgyaljon Japánnal xxxx tengeralattjáróink pár hónap múlva rákényszerítik Angliára a békét. Nyugtázza a vételt.

Fitz felnézett. Összeakadt a pillantása az ifjú Carverével, akiben, mint látta, forrt az izgalom.

Bizonyára az elfogott Zimmerman-üzenetet olvassa.

Valóban azt – felelte Fitz higgadtan. Ugyanolyan mámoros volt, mint Carver, de jobbnak látta palástolni. – Miért ilyen összefüggéstelen a megfejtett szöveg?

Ez egy új kód, amelyet még nem törtünk föl teljesen. De azért az üzenet óriási, nemde?

Fitz visszanézett a fordítására. Carver nem túloz. Ez nagyon úgy fest, mintha a németek meg akarnák szerezni szövetségesül Mexikót az Egyesült Államok ellen. Szenzációs!

Akár méregbe is hozhatja az amerikai elnököt annyira, hogy hadat üzenjen Németországnak." (Follett 2010)

Az üzenetet Alfred Zimmermann, német külügyminiszter küldte a mexikói német nagykövetnek 1917. január 19-én. A megfejtett változat hatalmas sajtónyilvánosságot kapott. Többen hamisnak vélték, ám Zimmermann megerősítette a híreszteléseket. Az addig nyugodtabb kedélyeket felborzolta a lehetséges támadások gondolata, így megváltozott az amerikaiak háborúhoz való hozzáállása. Míg 1914-ben ezerből ha egy ember gondolta volna, hogy háborúba lépnek, addig az üzenetet követően a többség sorsszerűnek ítélte a belépést. Ennek következtében 1917. április 6-án az USA hadüzenetet küldött a központi hatalmaknak, miután a képviselőház 373:50 arányban megszavazta azt. (Tarján)

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

5.8. A titkos kitevő

Sorra sikerrel győztétek le az elétek gördülő akadályokat. Ám a megpróbáltatásoknak még nem volt vége. A szörnyetegen átjutva az útvonalat követve egy hatalmas hegy széléhez értetek. Köd pihent a tájon. A távolban mintha valakinek a körvonalait fedeztétek volna fel. Egyre közeledett. Pár pillanat múlva egy fiatal hölgyre ismertek a homályos alakban. Egyenesen felétek tartott, pityeregve egy megsárgult papírlapot nyújtott oda nektek. Ezt olvastátok rajta: ,,Csodás dologra jöttem rá! Ha veszünk egy m számot, akkor mindig egy lesz a maradék m-mel osztva, ha bármely m-hez relatív prímet egy bizonyos kitevőre emelünk, méghozzá a következő kitevőre:...” — itt, a mondat végén elhalványult a papír, a kitevő értékét nem tudtátok kiolvasni. A hölgy így szólt: ,,Kedves Vándorok! Izabellának hívnak.” — örömittasan üdvözöltétek a lányt. Végre megtaláltátok! — ,,Édesapámtól maradt rám ez a módszer. De nem tudtam rájönni, hogy mire gondolhatott, és így nektek sem fogok tudni segíteni. Kérlek, fejtsük meg együtt, mert csak akkor tudom elárulni, hogy milyen titkosításra használta e felfedezést.” — mondta elhaló hangon. Egy percig sem tétlenkedtetek, azonnal nekiláttatok a rejtvénynek.

Segítő kérdéseken keresztül a feladat megoldása:

5.8.1. Hogy szól a matematika nyelvén a feladat?

Keressük x-et, hogy minden $(a, m) = 1$ esetén $a^x = k \cdot m + 1$.

,,Szerintem próbálkozzunk pár kisebb számmal, hátha rájövünk valamilyen logikára!” — javasolta Lajos.

Így először az $m = 5$-öt vizsgálták meg: tehát olyan x kell, hogy például 2^x, 3^x, 4^x, 6^x, 7^x is 1-et adjon maradékul 5-tel osztva.

Célszerű csak a maradékokkal számolni, ugyanis m^x — mivel m és x is nagyobb 1-nél — nagyon gyorsan nő, nagy számokkal pedig elég körülményes számolni. De hogyan használjuk a maradékokat? Én azt állítom, hogy ha k maradéka m-mel osztva d, akkor k^2 maradéka d^2. Nézzünk meg egy konkrét esetet! Legyen $k = 7$, $m = 5$, ekkor $d = 2$. $k^2 = 49$, 4 maradékot ad 5-tel osztva. $d^2 = 4$, ami szintén 4 maradékot ad 5-tel osztva. Nézzük meg általánosan! Az, hogy k maradéka m-mel osztva d, azt jelenti, hogy felírható $k = n \cdot m + d$ alakban. $(n \cdot m + d)^2 = (n \cdot m)^2 + 2n \cdot m \cdot d + d^2$, azaz d^2-en kívül minden tag osztható m-mel, tehát a maradék annyi lesz, amennyi d^2 maradéka. De mi a helyzet nagyobb hatványokkal? Láthatjuk, hogy ha a k^2 maradéka megegyezik d^2-ével, akkor az újabb hatványozásnál elég csak d^2-tel számolni. És itt mi történik? d^2-et megszorozzuk $n \cdot m + d$-vel, és ebben az egyedüli tag, amelyben nem szerepel az m szorzótényezőként az a d^3 lesz. Teljes indukcióval belátható, hogy ez bármely kitevőnél így működik, azaz k^x maradéka megegyezik d^x maradékával.

Készítsünk hozzá táblázatot, amelyben azt vizsgáljuk, hogy mennyi a^x 5-ös maradéka 5-höz relatív prímek esetén!

a^x	1	2	3	4	5
2	2	4	3	1	2
3	3	4	2	1	3
4	4	1	4	1	4
6	1	1	1	1	1
7	2	4	3	1	2

Ha megfigyeljük az oszlopokat, láthatjuk, hogy $x = 4$ esetén kapunk mindenhol 1-et maradékul. Ha ugyanezt eljátszuk $m = 3, 4, 5, 6, 7, 8, 9, 10$-re, akkor ezt tapasztaljuk:

n	3	4	5	6	7	8	9
x	2	2	4	2	6	2	6

„Hogy ez milyen ismerős!” — kiáltott fel hirtelen Hedvig. Lajos már mutatta is neki azt az előző számolást, ahol kipróbálták a relatív prímek kiszámolásához megtalált képletet. Majdnem teljesen megegyezett, csak a 8-nál szerepelt 2 helyett a 4, de mivel 4-ben megvan a 2, az előző logika alapján, ha a négyzetük 1 maradékot ad, akkor annak a négyzete 1^2, azaz 1 maradékot ad. „Ez nem lehet véletlen egybeesés...” — morfondírozott a fiú. — „Azt hiszem, a lekopott szöveg éppen $\varphi(m)$ lehetett. De ez még csak egy sejtés, a számok könnyen becsaphatnak. Nekünk bizonyosság kell.”

5.8.2. Hogyan tudnánk a sejtés alapján bizonyítást kreálni?

Azt kellene belátni tehát, hogy:

$$a \cdot a \cdot a \cdot ... \cdot a \cdot a = k \cdot m + 1,$$

ahol $\varphi(m)$ darab a-t szoroztunk össze. Biztosan kellenek majd az m-hez relatív prímek, hiszen nem lehet véletlen, hogy éppen annyi az a kitevője. Talán minden a-hoz kellene „csatolni” egy m-hez relatív prím számot? Nézzük meg!

Vegyük az összes m-nél kisebb és m-hez relatív prím számot, ezek legyenek r_1, r_2, r_3,..., $r_{\varphi(m)}$. Vizsgáljuk meg, hogy ezeket a-val megszorozva milyen maradékot kapunk!

$a \cdot r_i = k_i \cdot m + t_i$ — a kérdés, hogy t_i relatív prím m-hez, vagy sem. Tegyük fel, hogy nem. Ez azt jelenti, hogy van egy p prím, amelyik osztja m-et és t_i-t is, tehát a $k_i \cdot m + t_i$-t is. Azaz $a \cdot r_i$-t is osztania kellene. De egy prím csak akkor osztója egy szorzatnak, ha legalább egyik tényezőjének osztója. Mivel a és r_i is relatív prímek m-hez, így nem oszthatja egyik számot sem a p. Tehát a szorzatuk maradéka szintén m-hez relatív prím lesz.

A következő megfontolandó kérdés, hogy $a \cdot r_i$ és $a \cdot r_j$ (ahol $i \neq j$) adhat-e ugyanannyi maradékot m-mel osztva. Tegyük fel, hogy adhat.

Ez azt jelenti, hogy:

$$\text{I. } a \cdot r_i = k_i \cdot m + t_i$$

$$\text{II. } a \cdot r_j = k_j \cdot m + t_i.$$

A II. egyenletet az I.-ből kivonva ezt kapjuk:

$$a \cdot (r_i - r_j) = (k_i - k_j) \cdot m$$

Mivel $(a, m) = 1$, így annak kellene teljesülnie, hogy m osztja $r_i - r_j$-t, azaz:

$$r_i - r_j = k_{ij} \cdot m,$$

tehát:

$$r_i = k_{ij} \cdot m + r_j.$$

De mivel feltettük, hogy r_i és r_j különböző maradékok, ez nem teljesülhet. Tehát minden szorzatunk különböző, m-hez relatív prím maradékot ad, és mivel annyi szorzatunk van, ahány m-nél kisebb m-hez relatív prím szám, így a maradékok r_1-et, r_2-t, ... , $r_{\varphi(m)}$-et fogják kiadni valamilyen sorrendben. Ez azért jó nekünk, mert ha ezeket az egyenleteket összeszorozzuk, akkor a bal oldalon a-nak éppen a $\varphi(m)$-edik hatványa jelenik meg, és mindkét oldalon ugyanazokat a maradékokat szorozzuk össze.

A jobb oldal maradékát még meg kell gondolnunk.

$$(k_1 \cdot m + t_1) \cdot (k_2 \cdot m + t_2) \cdot ... \cdot (k_{\varphi(m)} \cdot m + t_{\varphi(m)}),$$

ahol t_1, t_2, ... , $t_{\varphi(m)}$ az r_1, r_2, ... , $r_{\varphi(m)}$ egy sorbarendezése.

A szorzatban az m-es tagok mind nullát adnak maradékul, így egyedül az m-et nem tartalmazó tag lesz érdekes. Ez a t-k szorzata. Tehát a jobb oldal így írható fel: $k \cdot m + t_1 \cdot t_2 \cdot ... \cdot t_{\varphi(m)}$.

A bal és jobb oldal együtt:

$$a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdot ... \cdot r_{\varphi(m)} = k_0 \cdot m + r_1 \cdot r_2 \cdot ... \cdot r_{\varphi(m)}$$

Legyen $r_1 \cdot r_2 \cdot ... \cdot r_{\varphi(m)} = l \cdot m + d$, ekkor:

$$a^{\varphi(m)} \cdot (l \cdot m + d) = k_0 \cdot m + l \cdot m + d$$

Ez akkor teljesül, ha

$$a^{\varphi(m)} \cdot d = k_d \cdot m + d$$

$$(a^{\varphi(m)} - 1) \cdot d = k_d \cdot m$$

Mivel d az m-nél kisebb, m-hez relatív prím számok szorzatának maradéka, így a fent már megmutatottak alapján ez biztosan relatív prím m-hez. Ebből az következik, hogy $a^{\varphi(m)} - 1$-nek oszthatónak kell lennie m-mel, azaz:

$$a^{\varphi(m)} - 1 = k \cdot m$$

Azaz:

$$a^{\varphi(m)} = k \cdot m + 1$$

És éppen ezt akartuk belátni. Tehát a lekopott hatványkitevő valóban a $\varphi(m)$.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

A behelyettesítés vesztesei

Tudatlansága miatt került kellemetlen helyzetbe II. Fülöp spanyol király a 16. században. A francia uralkodóknak, III. Henriknek és IV. Henriknek dolgozó, mára már formulájáról ismert matematikus, François Viète okozott Fülöpnek fejtörést. Ugyanis Viète előszeretettel fejtette meg a spanyolok ,,elcsípett" titkos üzeneteit. Olyan eredményes volt, hogy II. Fülöp megelégelte. Ördögi terve szerint bemószerolta Viète-et a Vatikánban, mondván, hogy itt mágiáról van szó, csupán boszorkánysággal magyarázható ez a jelenség. A Vatikánban azonban nem François-t ítélték égetni valónak, hanem Fülöpöt égetni való bolondnak: ugyanis a Pápai Állam, titkosító és titokfejtő paradicsomként, szintén könnyedén megfejtette a spanyol behelyettesítéssel íródott üzeneteket. Így II. Fülöpön és a spanyolokon szórakozott a korabeli Európa krémje. (Singh 2001: 37–38)

I. Mária skót királynő azonban Fülöpnél rosszabbul járt. Az Anglia és Skócia között dúló hatalmi harcok, illetve vallási ellentétek egyébként is jelentősen megnehezítették az élete során koronájától megfosztott, többször bebörtönzött Máriát. A korona visszaszerzésére tett sikertelen kísérlet után Skóciából Angliába menekült, ahol I. Erzsébetnél, unokanővérénél kívánt megbújni. Ám az angol királynő nem kegyelmezett: bebörtönözte. Itt Mária különböző összeesküvésekben vett részt, s erről számtalan titkos levelet váltott cinkosaival. Ezekben kódszavakat is használt, illetve nullitásokkal, azaz üres karakterekkel, igyekezett nehezíteni a feltörést. Ám szerencsétlenségére ezek a levelek mind-mind I. Erzsébet kódfejtőinél kötöttek ki, akik hamar rájöttek, hogy a királynő meggyilkolásán mesterkednek Máriáék. A leleplezés nem volt elég, az összeesküvők teljes névsorát akarták: így a megfejtett módszerrel hamisítottak Mária nevében a levélre egy utóiratot, melyben a terv résztvevőinek nevét kéri. Máriát halálra ítélték, 1587. február 8-án lefejezték. (Singh 2001: 41–52)

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

5.9. Lakat a számon

,,Fantasztikus! Fantasztikus!" — lelkendezett Izabella. — ,,Már csak pár homályos folt maradt! Viszont ahhoz, hogy elmondjam, néhány dolgot végig kell gondolnotok, különben nem fogjátok megérteni. Íme az első feladványom: Eddig a titkos információt egy megbízhatónak hitt futárral küldtétek egymásnak. Ám róla kiderült, hogy kíváncsibb a kelleténél, és ellopja azt, ami nincs lezárva. Van egy lakattal zárható ládátok. Nektek is van egy lakatotok és egy kulcsotok, illetve a csoport másik felének is, viszont a ti kulcsotok nem nyitja a másik lakatot, az ő kulcsuk pedig nem nyitja a ti lakatotokat. Hogyan juttatjátok el a titkos üzenetet a kíváncsi futárral, akinek egyik lakathoz sincs kulcsa?"

Segítő kérdéseken keresztül a feladat megoldása:

5.9.1. Hogyan álljunk neki a lehetetlennek tűnő feladatnak?

Tudjuk, hogy van nálunk egy láda, egy lakat, egy üzenet, és nekünk kell elindítani a cserét. Gondoljuk végig, hogy milyen lépés lehet az első! Küldhetjük nyitva üresen, zárva üresen, nyitva üzenettel, zárva üzenettel a ládát. Küldhetjük csak a lakatot vagy csak az üzenetet, esetleg a lakatot és az üzenetet együtt.

Rövid gondolkodás után belátható, hogy az üzenet védtelenül nem küldhető. A lakat átküldése üzenet nélkül szintén nem járható, hiszen akkor utána valamikor megint védtelenül kellene átküldenünk az üzenetet. Ha csak a ládát küldjük, akkor a másik csapat nem tud jól lépni (vagy visszaküldik, vagy ráteszik a lakatot, így viszont mi nem tudjuk betenni az üzenetet).

Így az egyedüli útnak az látszik, ha az üzenetet a lezárt ládában átküldjük. A többiek mit léphetnek erre? Kinyitni nem tudják, viszont a lakattal cselezhetnek. Ha úgy teszik a ládára, hogy a mi lakatunkon és a záron is átkulcsolják, akkor nyert ügyünk lesz. Hiszen ha visszakapjuk, akkor a saját lakatunkat kinyithatjuk, levehetjük. Ekkor a láda zárva marad, hiszen a másik csapat lakata rajta van még. Visszaküldjük, ők pedig ki tudják nyitni. A kíváncsi futár pedig nem látott semmit.

5.9.2. Mi a helyzet, ha a lakatokat nem fizikai értelemben képzeljük el, hanem úgy mint kódolási szabályokat?

Ha ráteszem, az azt jelenti, hogy az üzenetet a saját hozzárendelésem szerint kódoltam, ha leveszem, akkor a kapott üzenetet a saját hozzárendelésem inverzével dekódolom. De ez működhet? Nézzük meg!

5.10. A kíváncsi matekos futár

„Ügyesek vagytok! Ez könnyen ment, úgyhogy jöjjön egy nehezebb: az eddigi futárunkról kiderült, hogy kíváncsiságánál csak matektudása nagyobb. Most nincs lakat, nincs láda, csupán két csapat. Az egyik fele szeretne egy fontos üzenetet átjuttatni a másiknak. A megfeleltetéses kódolás mikor alkalmazható? Lehet úgy csinálni, hogy nincs közös titok az ügy lefolytatásakor?”

Segítő kérdéseken keresztül a feladat megoldása:

5.10.1. Segíthet, ha leegyszerűsítjük a kérdést és matematikai köntösbe bújtatjuk!

Legyen a titkos üzenet egy szám az egyszerűség kedvéért, jelöljük x-szel. Az egyik csapat kódolási eljárása legyen $f(x)$, a másiké $g(x)$. Az előzőekben láthattuk, Jani ötleténél, hogy invertálható függvényekre van szükségünk, azaz létezik $f^{-1}(x)$ és $g^{-1}(x)$.

Tehát a lakatos feladat analógiája szerint így nézne ki a tranzakció:

A csapat ,,ráteszi a lakatot”:	A csapat $\rightarrow f(x) \rightarrow$ B csapat
B csapat is ,,ráteszi a lakatot”:	A csapat $\leftarrow g(f(x)) \leftarrow$ B csapat
Az A csapat ,,leveszi a lakatot”:	A csapat $\rightarrow f^{-1}(g(f(x))) \rightarrow$ B csapat
B csapat is ,,leveszi a lakatot”:	B csapat: $g^{-1}(f^{-1}(g(f(x))))$

Elvileg ez után a művelet után x-et, azaz a titkos üzenetet kellene megkapnia.

5.10.2. Ez minden invertálható f és g esetén így van? Próbáljuk ki!

Legyen $f(x) = x + 2$ és $g(x) = 3x$, ekkor $f^{-1}(x) = x - 2$ és $g^{-1}(x) = \frac{x}{3}$

Ekkor így nézne ki az üzenetküldés, ha a titkos üzenet 7:

1. lépés:	A csapat $\rightarrow 9 \rightarrow$ B csapat
2. lépés:	A csapat $\leftarrow 27 \leftarrow$ B csapat
3. lépés:	A csapat $\rightarrow 25 \rightarrow$ B csapat
4. lépés:	B csapat: $\frac{25}{3} \neq 7$

Láthatjuk, hogy erre a két függvényre nem működött a módszerünk. Mi lehetett a hiba?

5.10.3. Milyen elsőfokú függvénypárok lesznek alkalmasak? Gondoljuk végig általánosan!

Legyen $f(x) = ax + b$ és $g(x) = cx + d$. Ekkor $f^{-1}(x) = \frac{x-b}{a}$ és $g^{-1}(x) = \frac{x-d}{c}$

Ekkor így nézne ki az üzenetküldés, ha a titkos üzenet x:

1. lépés:	A csapat $\rightarrow ax + b \rightarrow$ B csapat
2. lépés:	A csapat $\leftarrow c(ax + b) + d \leftarrow$ B csapat
3. lépés:	A csapat $\rightarrow \dfrac{c(ax + b) + d - b}{a} \rightarrow$ B csapat
4. lépés:	B csapat: $\dfrac{\frac{c(ax+b)+d-b}{a} - d}{c}$

Mikor működik ez a módszer? Ha a végén B az x-et kapja vissza. Tehát teljesülnie kell a következő egyenletnek:

$$\frac{\frac{c(ax+b)+d-b}{a} - d}{c} = x$$

c-vel és a-val való szorzás után ezt kapjuk:

$$cax + cb + d - b - da = cax$$

Azaz:

$$cb - b = da - d,$$

tehát ha a, b, c és d kielégítik a következő egyenletet, akkor működik a módszerünk:

$$a = \frac{cb - b}{d} + 1.$$

5.10.4. Próbáljuk ki!

Legyen $b = 3$, $c = 2$, $d = 1$, ekkor $a = 4$. Tehát $f(x) = 4x + 3$, $g(x) = 2x + 1$, $f^{-1}(x) = \frac{x-3}{4}$ és $g^{-1}(x) = \frac{x-1}{2}$

Tehát a tranzakció:

1. lépés:	A csapat $\rightarrow 4x + 3 \rightarrow$ B csapat
2. lépés:	A csapat $\leftarrow 2(4x + 3) + 1 = 8x + 7 \leftarrow$ B csapat
3. lépés:	A csapat $\rightarrow \frac{8x+7-3}{4} = 2x + 1 \rightarrow$ B csapat
4. lépés:	B csapat: $\frac{2x+1-1}{2} = x$

Tehát valóban megtudta a B csapat, hogy mi volt a titkos üzenet.

5.10.5. Egy kérdés még maradt: legfeljebb mennyit tudhat a minden hájjal megkent futár, hogy a titkot biztosan ne tudja kitalálni?

Akkor ki tudja találni az üzenetet, ha csak azt látja, amit egymásnak üzennek a felek, és annyit tud, hogy mindkét csapat elsőfokú függvényeket használ?

Tegyünk egy próbát! Ki tudod találni a két függvényt, ha futárként a következő üzenetváltást közvetíted?

1. lépés:	A csapat $\rightarrow 22 \rightarrow$ B csapat
2. lépés:	A csapat $\leftarrow 67 \leftarrow$ B csapat
3. lépés:	A csapat $\rightarrow 13 \rightarrow$ B csapat

Mit tudunk meg ebből?

$$\text{I. } ax + b = 22$$

$$\text{II. } c(ax + b) + d = 67$$

$$\text{III. } \frac{c(ax+b)+d-b}{a} = 13$$

Az első összefüggést a másodikba helyettesítve ezt kapjuk:

$$c \cdot 22 + d = 67 \rightarrow d = 67 - c \cdot 22$$

A második összefüggést a harmadikba írva pedig erre jutunk:

$$\frac{67 - b}{a} = 13 \rightarrow b = 67 - 13a$$

Ezt az első egyenletbe helyettesítve és a-ra rendezve a következőt kapjuk:

$$a = \frac{45}{13 - x}$$

Ez esetben, még ha diofantoszi egyenletnek is kezeljük, akkor is több megoldás lehetséges, például x lehet -2 is, 4 is, 8 is, 10 is. Ha pedig nem diofantoszi az egyenletünk, azaz az üzenetre és a függvényünk együtthatóira sem teszünk megkötést, akkor végtelen sok x jöhet szóba. Tehát a futár nem jöhet rá az üzenetünkre. Ám ekkor az együtthatókra vonatkozó összefüggést titkosan kellett egyeztetnünk. Mi a helyzet, ha arról is tud?

Ekkor az előzőeket még annyival kell kiegészíteni, hogy:

$$a = \frac{cb - b}{d} + 1.$$

Ha ebbe behelyettesítjük a fentiekben b-re és d-re kapottakat akkor a következő egyenletet kapjuk:

$$a = \frac{(67 - 13a)(c - 1)}{67 - 22c} + 1,$$

ami szintén végtelen sok megoldást szolgál (ha nem az egészek körében keressük). Viszont egészek esetén sajnos a csalafinta futár leszűkítheti az üzenetek körét véges sok esetre.

5.11. A hihetetlen titkosító eljárás

A fiatal hölgy arca felderült. Csak ámult és bámult, a sok tehetség láttán. Érdemesnek talált benneteket arra, hogy elmondja az eljárást: ,,Édesapám sokat gondolt a bajra. Így kitalált egy olyan módszert, amihez nem kell titkos üzeneteket küldenünk egymásnak: ő mindenki füle hallatára elmond két számot, én ezek segítségével titokba burkolom üzenetemet, ezt viszont csak ő fogja tudni kibogozni." Hedvigék alig hittek a fülüknek. ,,Ennek az egyik kulcsa az, amit ti megfejtettetek. Látom, jól vág az eszetek, és nem tennétek rosszat nekem. Így elárulom. Azért is, mert van benne még egy-két homályos folt. Segíthetnétek azt is tisztázni!" Lajosék lelkesen bólogattak, izgatottan várták a csodát. ,,De készüljetek fel, bonyolult lesz!" — figyelmeztetett a hölgy.

5.11.1. "Először egy feladványt kaptok: ha el akarjuk dönteni 1291-ről, hogy prím-e, akkor meddig kell ellenőrizni az oszthatóságot?" — Kérdezte kacsintva Izabella.

Gyorsan nézzük meg, hogy a kisebb prímek közül osztja-e valamelyik! Látható, hogy 2-vel, 3-mal, 5-tel nem osztható. Számológéppel ellenőrizhetjük tovább, elmehetünk 29-ig is, de egyik sem osztja. Tehát az az út nem járható, hogy gyorsan megtaláljuk az egyik osztóját. Inkább egy általánosabb elvet kellene megnéznünk!

A csapat ezt gondolta végig: nézzük meg, hogy mi történik, ha egy számnak megtaláljuk az egyik osztóját! Például látjuk, hogy a 305-nek osztója az 5, ám ez egyúttal azt is jelenti, hogy a 305-nek a $\frac{305}{5} = 61$ is osztója. Ezek osztópárt alkotnak. Ha megnézzük egy szám egyik osztópárját, akkor vagy az egyik szám nagyobb a másiknál, vagy ugyanakkora a két szám (négyzetszámok esetén létezik csak ilyen osztópár). De az biztos, hogy ha az egyik felével osztható, akkor a másikkal is. Mi következik ebből? Ha szépen sorban ellenőrzöm, hogy a bizonyos szám osztható-e 2-vel, 3-mal, 5-tel, 7-tel, és így tovább az egymást követő prímeket veszem, akkor, ha felteszem, hogy p osztja N-t, akkor $\frac{N}{p}$ is osztja. Viszont azon prímeket nem kell leellenőrizni, amelyekhez biztosan kisebb osztópár jutott volna, hiszen akkor a kisebbnél már megkaptuk volna osztóként. De mely prímekről tudhatjuk egy N szám láttán, hogy biztosan az osztópár nagyobbik tagjai lesznek?

Nézzünk meg egy olyan N-t, amelyiknek sok osztópárja van, hátha meglátunk valamit! Legyen $N = 144$.

$$N = 144 = 1 \cdot 144 = 2 \cdot 72 = 3 \cdot 48 = 4 \cdot 36 = 6 \cdot 24 = 8 \cdot 18 = 9 \cdot 16 = 12 \cdot 12$$

A bal oldalon lévő számok sorra nőnek, míg a jobb oldalon lévők sorra csökkennek. Bal oldalon csak 12-ig kellett mennünk, hiszen az annál nagyobb osztók, mint például a 16, már szerepelnek a felsorolásban, hiszen a párjuk kisebb volt. De a 12-nek mi a kitüntetett szerepe? Amellett, hogy az a legutolsó a felsorolásban, a párja ,,saját maga". Tehát a 12 a 144 gyöke. Akkor lehet, hogy csak a gyökig kell ellenőrizni? Tegyük fel, hogy találunk olyan p prímosztót, amelyik nagyobb N négyzetgyökénél, és az osztópárja, legyen q is nagyobb N négyzetgyökénél.

Ekkor az teljesülne, hogy $p \cdot q = N = \sqrt{N} \cdot \sqrt{N}$. Tehát két $\sqrt{N}$-nél nagyobb szám szorzata egyenlő lenne $\sqrt{N}$-nek önmagával vett szorzatával. Ám ez ellentmondás. Tehát azt látjuk, hogy $\sqrt{N}$-ig kell megvizsgálni. De mi a helyzet, ha egy szám gyöke nem egész? Például a 28? Akkor a gyök egészrészéig kell csak megnézni, hiszen az azt követő egész már nagyobb, mint $\sqrt{N}$, és akkor az előző gondolatmenet alapján már nem kell ellenőrizni. Tehát 27 esetén elég csak 5-ig ellenőrizni.

Így a feladatunk: 1291-ről eldönteni, hogy prím-e. Ehhez először szüség van a gyökére: $\sqrt{1291} \approx 35,93$. Tehát 35-ig kell ellenőriznünk. Ez azt jelenti, hogy megnézzük, hogy 2-vel, 3-mal, 5-tel, 7-tel, 11-gyel, 13-mal, 17-tel, 19-cel, 23-mal, 29-cel és 31-gyel osztható-e. Láthatjuk, hogy nem, tehát az 1291 prím.

,,Már ebből az eljárásban is látható, hogy habár csak a gyökig kell ellenőrizni, ez nagy számok esetén rengeteg prímet jelent, még a gépeknek is gondot okot." — osztotta meg veletek Izabella a megfejtés elismeréseként.

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

Gárdonyi Géza titkos naplója

Gárdonyi naplóját titkosírással írta, s habár egyszerű módszert alkalmazott, a betűket különböző jelekkel helyettesítette, mégis komoly fejtörést okozott a lelkes érdeklődőknek. Többen tébolyultsággal vádolták, ám amikor az író halála után majd' ötven évvel megfejtették a rejtélyt, látták, hogy rendszer van Gárdonyi tömérdek titkos feljegyzése mögött. Titkosnapló címen kiadták ezeket a ,,lefordított" szövegeket. Az előszóban Z. Szalai Sándor így ír a megfejtésről: ,,A megváltozott körülmények között — a munka anyagi és erkölcsi feltételeit megteremtő egri múzeum felhívására — huszonketten jelentkeztek a különös-ritka hagyaték ismeretlen tartalmának földerítésére. Tanárok, diákok, munkások, orvosok, közgazdászok, tisztviselők és mások; a titkosírásos rendszerek-formák ismerete vonatkozásában laikusok és szakképzett kutatók. Gilicze Gábor (egyetemi hallgató) a Füles rejtvényújságból, Gyürk Ottó (honvéd alezredes) egy televíziós vetélkedőből értesült a szokatlan feladatról. A két sikerrel járt megfejtő különböző módon közelített tárgyához (az egyik segédeszközök nélkül, a másik a korszerű technikát hívta segítőtársául), s fölfedezéseik egy napon egybehangzottak." (Gárdonyi 1974)

♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠ ♣♢♡♠

5.11.2. Mert kell egy N, hol egy prímszám sem látható!

Izabella elmondta, hogy először is szükségünk lesz egy számra, N-re, amely két nagyon nagy, 2-300 jegyből álló prím szorzata. Ez azért volt fontos, mert csak N-t lehet elmondani, viszont mivel hatalmas számról van szó, így senki sem ismerte a prímfelbontását, csak mi. ,,És azt is csak mi tudjuk majd, hogy N-ig hány darab relatív prím található!" — örvendezett Hedv-ig. ,,Rátapintottál a lényegre." — mondta elismerően a hölgy. ,,De erre majd kicsit később térünk ki."

,,Ez szép és jó, de honnan szerzünk ilyen hatalmas prímszámokat?" — kérdezett vissza Lajos. Izabella elmesélte, hogy elég hatékony prímteszteket ismerünk, azaz olyan teszteket, amelyek gyorsan kizárják az összetett számokat. Használjuk csak fel, amit kitaláltunk! Tudjuk, hogy egy p prím esetén $\varphi(p) = p - 1$, és tudjuk, hogy minden $p > 2$ esetén $(p, 2) = 1$, azaz felhasználva a kitalált tételünket 2^{p-1} mindenképpen 1 maradékot ad p-vel osztva. Ebből következik, hogy ha 2^{n-1} maradéka nem 1 n-nel osztva, akkor n biztosan összetett, ha pedig 1, akkor ,,szinte biztosan" prím. Ezen kívül azt is biztosan tudjuk, hogy ,,elég sok" prímszám áll rendelkezésünkre. A prímszámtétel alapján kiszámolhatjuk, hogy körülbelül minden 345-ödik 300-jegyű páratlan szám prím, és például a hárommal oszthatóak azonnal kizárhatók (Freud – Gyarmati 2006: 217). Így viszonylag gyorsan találhatunk ilyen prímeket

5.11.3. Hogyan fogjuk be- és kicsomagolni az üzenetet?

Hiszen, ahogy már tapasztalhatta csapatunk, szükség lesz egy módszerre, amellyel a küldő ,,becsomagolja" az üzenetet, és szükség lesz egy módszerre, amellyel a fogadó ,,kicsomagolja" azt. Azaz a matematika nyelvén: kell egy függvény, amelynek létezik az inverze. A függvényt mindenki ismeri, az inverzét viszont csak mi.

Ez hogyan lehetséges? És hogyan jönnek a képbe a prímek, a relatív prímek? ,,Biztosan valamilyen hatványos-maradékos dolog lesz!" — kiáltott Hedvig. ,,Miből gondolod?" - kérdezte Izabella. ,,Hát mondtad, hogy a relatív prímes megoldás kelleni fog még valamire. Ráadásul egy ilyen bonyolult függvénynek biztos nehét megtalálni az inverzét." — gondolkodott hangosan Hedvig. Izabella bólogatott, és elmondta, hogy mire jutott az édesapja.

Izabella azzal kezdte, hogy az egyszerűség kedvéért vegyük az N számot egy konkrét értéknek, azt mondta, hogy legyen $N = 3 \cdot 11 = 33$. Jelöljük T-vel a függvényünket, ami valóban ,,hatványozós-maradékos" lesz, ahogy Hedvig sejtette. Legyen r az üzenetünk, ami az az N-nél kisebb szám, amit a másiknak meg akarunk ,,súgni". Most legyen $r = 8$. Kell egy kitevő, amire az r-t emeljük. Ezt jelöljük t-vel, ennek azt kell teljesítenie, hogy $(\mathrm{t}, \varphi(N)) = 1$. Jelen esetben $\varphi(n) = (3-1)\cdot(11-1) = 20$, így legyen $t = 7$. Ekkor a ,,csomagolós" függvényünk a következőképpen nézzen ki:

$T(r) = r^t$ **legkisebb pozitív maradéka** N **szerint.**

Azaz a példánkban (ami természetesen a valóságban nem alkalmas, hiszen nagyon könnyen felbontható, kitalálható):

$T(8) = 8^7$ legkisebb pozitív maradéka 33 szerint: $8^7 = 2097152 = 63550 \cdot 33 + 2$

Most kellene hozzá egy ,,kicsomagolós" függvény is. Érdemes hasonló alakban keresni, azaz:

$M(s) = s^m$ **legkisebb pozitív maradéka** N **szerint.**

Tehát annak kell teljesülnie, hogy

$r = TM(r) = MT(r) = r^{tm}$ **legkisebb pozitív maradéka** N **szerint.**

Tehát r és r^{tm} ugyanazt a maradékot adják N szerint.

5.11.4. Milyen kitevőre emeljük, hogy ugyanaz legyen a maradék?

,,Apa azt írta, hogy az $1 + k \cdot \varphi(N)$ **megfelelő lesz** tm**-nek, de én még nem tudom, hogy miért. Ti esetleg rá tudtok jönni?" — kérdezte tanácstalanul Izabella.**

„Én tudom!” – kiáltotta Hirtelen Hedvig. – „Az a kérdés, hogy $r^{1+k\varphi(N)}$ ugyanannyit ad-e maradékul N-nel osztva, mint r. Mi sem egyszerűbb ennél: $r^{1+k\varphi(N)} = r \cdot r^{k\varphi(N)}$az előbb beláttuk, hogy $r^{\varphi(N)}$ 1-et ad maradékul, ha azt megszorozzuk r-rel, akkor valóban r lesz a maradék!” Lajos a homlokát ráncolta: „Óvatosab-ban azzal a fejszével, Hedvig! Lassan a testtel! A mi bizonyításunk azt mondta, hogy olyan r-ekre működik, amelyek relatív prímek. Viszont ez most nem biztos. Szóval itt valamit azért még cseleznünk kell, habár kiindulásnak jó lesz, amit mondtál.”

Tehát továbbgondolták Hedvig ötletét. Eddig rendben volt:

$$r^{1+k\varphi(N)} = r \cdot r^{k\varphi(N)} = r \cdot (r^{\varphi(N)})^k$$

Ezen kívül tudjuk, hogy $N = p \cdot q$, ahol p és q prímek. Hogyan tudnánk akkor felírni az N-hez relatív prímek számát? A megtalált képletet N-re alkalmazva:

$$\varphi(N) = (p-1) \cdot (q-1)$$

És prímek esetén mennyi ez az érték? Akár a képletet, akár józan eszünket használva: $1, 2, 3, ..., p$ közül egyedül p az, amelyik nem relatív prím p-hez, az összes többi szám az, így minden p prímre $\varphi(p) = p - 1$. Ez alapján a fenti képletet továbbfejthetjük:

$$\varphi(N) = (p-1) \cdot (q-1) = \varphi(p) \cdot \varphi(q)$$

Tehát:

$$r^{1+k\varphi(N)} = r \cdot r^{k\varphi(N)} = r \cdot (r^{\varphi(p)\cdot\varphi(q)})^k$$

Azt kell belátnunk, hogy ha b egy tetszőleges egész, akkor:

$$r \cdot (r^{\varphi(p)\cdot\varphi(q)})^k = b \cdot N + r$$

Átrendezés és kiemelés után:

$$r \cdot [(r^{\varphi(p)\cdot\varphi(q)})^k - 1] = b \cdot N$$

Mivel $N = p \cdot q$ és $(p, q) = 1$, így azt kell belátnunk, hogy a bal oldal osztható p-vel is és q-val is.

Első: p-vel való oszthatóság

I. eset: $(r, p) \neq 1$, azaz r osztható p-vel: ekkor a bal oldal nyilván osztható p-vel.

II. eset: $(r, p) = 1$

$$r \cdot [(r^{k\cdot\varphi(q)})^{\varphi(p)} - 1] = b \cdot q \cdot p$$

Mivel r és p relatív prímek, ezért $r^{\varphi(p)}$ 1-et ad maradékul p-vel osztva, így $(r^{k\cdot\varphi(q)})^{\varphi(p)}$ is 1-et ad maradékul, amelyből 1-et kivonva egy p-vel oszható számot kapunk.

Második: q-val való oszthatóság

Az előző eset alapján végiggondolható, látható, hogy a q-val való oszthatóság is rendben van.

Tehát tudjuk, hogy a bal oldal minden r esetén osztható p-vel és osztható q-val is. Mivel $(p, q) = 1$, így osztható $p \cdot q$-val, azaz N-nel is, tehát beláttuk az állítást.

5.11.5. Mindig megoldható az egyenlet?

Izabella szeme csillogott a boldogságtól. Érezte, hogy már közel a teljes megoldás. Már csak azt kellett tisztázni, hogy ha adott t, adott N, akkor mindig egész lesz-e az m a $tm = 1 + k \cdot \varphi(N)$ egyenlet alapján. Izabella édesapja feltehetőleg erre jutott, de még nem tudhatták biztosan a fiatalok. Így Lajosék nekiláttak a problémának.

Tehát m-et így kaphatjuk meg:

$$m = \frac{1 + k \cdot \varphi(N)}{t}$$

Azt tudjuk, hogy t és $\varphi(N)$ relatív prímek. Akkor kaphatunk egész m-et, ha az $1 + k \cdot \varphi(N)$ osztható t-vel, azaz ha a $k \cdot \varphi(N)$ maradéa $(t-1)$ lesz t-vel osztva. Lőjünk ágyúval verébre, ha már olyan jól kitaláltuk a tételünket. Azt tudjuk, hogy $(\varphi(N), t) = 1$ miatt $[\varphi(N)]^{\varphi(t)}$ 1-et ad maradékul t-vel osztva. Azaz ezt $(t-1)$-gyel szorozva olyan számot fogunk kapni, ami $t-1$-et ad maradékul. De ehhez milyen k szükséges? Az alábbi okoskodás alapján felírható:

$$k \cdot \varphi(N) = [\varphi(N)]^{\varphi(t)} \cdot (t-1)$$

$$k = [\varphi(N)]^{\varphi(t)-1} \cdot (t-1)$$

esetén biztosan egész lesz az m. (Mivel az eredeti egy diofantikus egyenlet, így az euklideszi algoritmust alkalmazva ennél sokkal gyorsabban eredményre jutunk, és egy jóval kisebb m-et kapunk, ami a gyakorlati alkalmazás esetén rendkívül fontos, a lenti példában mi is azzal számolunk. Emellett a fenti számolás $\varphi(t)$ miatt is problematikus lehet, hiszen előfordulhat, hogy t prímtényezős felbontását sem ismerjük.) Tehát megalkottuk az inverzfüggvényt, amihez tényleg szükséges N prímtényezős felbontása, hiszen $\varphi(N)$ csak annak ismeretében számolható ki.

5.11.6. Mit üzen nekünk RSA?

Térjünk vissza a példánkra, hogy azon keresztül kipróbálhassuk!

Tehát a példánkat a következő számokkal vizsgáljuk meg:

$N = 3 \cdot 11 = 33$
$\varphi(N) = 2 \cdot 10 = 20$
$r = 8$
$(t, \varphi(N)) = 1$, $t = 7$
$T(r) = r^t$ legkisebb pozitív maradéka N szerint,
mivel $T(8) = 8^7 = 2097152 = 63550 \cdot 33 + 2$ legkisebb pozitív maradéka N szerint,
így $T(8) = 2$
$M(s) = s^m$ legkisebb pozitív maradéka N szerint,
ahol azt tudjuk, hogy $tm = 1 + k \cdot \varphi(N)$, azaz:

$$7 \cdot m = 1 + k \cdot 20$$

$$m = \frac{20 \cdot k + 1}{7} = 3 \cdot k + \frac{1 - k}{7}$$

mivel az $f(k) = 20 \cdot k + 1$ szigorúan monoton növekedő és m pozitív, így a lehető legkisebb olyan k-t keressük, amelyre m pozitív egész. Mivel a 0-nak minden szám osztója, így legyen $1 - k = 0$, azaz $k = 1$, azaz $m = 3$.

Tehát $M(s) = s^3$ legkisebb pozitív maradéka 33 szerint.

Ezek alapján hogyan is megy az üzenet kitalálása? Rejtelmes Sehollakó Anonymusszal (röviden RSA-val) fogunk nyilvánosan kommunikálni:

1. lépés	Mi közzétesszük azt, hogy $N = 33$, $t = 7$ és a T függvényt
2. lépés	RSA ez alapján kiszámolja, hogy $T(8) = 2$ és közzéteszi
3. lépés	$M(T(8)) = M(2) = 8$ alapján megkaptuk az üzenetet.

Így Rejtelmes Sehollakó Anonymus meg tudta üzenni nektek a kódot (most képzeljük azt, hogy N két hatalmas prímszám szorzata volt). Indulhattatok is a kincshez. A megadott koordináták alapján pár órányi gyalogtúra után, ami a magatok mögött hagyott veszedelmekhez képest igazán semmiségnek tűnt, odaértetek. Egy palotában őrizték. Kapujában egy égő fáklya fogadott titeket. Így szólt: ,,Fogjatok, s tüzemmel égessétek a kódot a kapuba!" — Hedvig és Lajos megfogták a fáklyát, és egy gyönyörű nyolcast kanyarítottak az ezeréves ajtóba. A nyolcas csodák csodájára nyolcat pördült, majd fekve állt meg. Nagy nyikorgás közepette kinyílt a bejárat. Egy végeláthatatlan csigalépcső előtt találtátok magatokat. Felfutottatok a tetejére, ahol egy csodakút várt titeket. Aki belenézett, bármit kívánt, előbb vagy utóbb valóra vált.

Vége

6. Irodalomjegyzék

- Czeizel Endre 2011. *Matematikusok, gének, rejtélyek.* Galenus Kiadó. Budapest.

- Csirmaz László 2005. Kriptográfia a középiskolában. *A matematika tanítása: módszertani folyóirat* 2: 3–13.

- Erdős Pál 1993. *Gólyavári előadás.* ELTE. Budapest.

- Erdős Pál 1997. Hogyan lettem matematikus és világvándor? *Természet Világa* 2: 78–79.

- Follett, Ken 2010. *A titánok bukása - Évszázad-trilógia 1.* Gabo Könyvkiadó. Budapest.

- Freud Róbert – Gyarmati Edit 2006. *Számelmélet.* Nemzeti Tankönyvkiadó. Budapest.

- Gárdonyi Géza 1974. *Titkosnapló.* Szépirodalmi Kiadó. Budapest.

- Gerőcs László – Orosz Gyula – Paróczay József – Szászné Simon Judit 2006. *MATEMATIKA Gyakorló és érettségire felkészítő feladatgyűjtemény I.* Nemzeti Tankönyvkiadó. Budapest.

- Jéki László 2004. Megfejtem Makk ezredes titkosírását. *Ponticulus Hungaricus* 10.

- Jókai Mór 2001. *A mi lengyelünk, Jókai összes művei.* Arcanum. Budapest.

- Juhász Péter 2010. *„Hogyan foglalkozzunk tehetséges gyerekekkel?" című szemináriumon.* Szóbeli közlés, ELTE TTK. Budapest.

- Kosztolányi József – Kovács István – Pintér Klára – Urbán János – Vincze István 2007. *Sokszínű matematika - tankönyv 9. osztály.* Mozaik Kiadó. Szeged.

Kuczka Péter 2011. A szórakozás értelme. *Határvidék – A science fictiontől a barkochbáig.* Digitális Irodalmi Akadémia, Petőfi Irodalmi Múzeum. Budapest.

- Markó Tamás (szerk.) 1996. *A számítástechnika története.* Janus Pannonius Tudományegyetem. Pécs.

- Neumann János 1972. *A számológép és az agy.* Gondolat Kiadó. Budapest.

- Róka Sándor 2006. *2000 feladat az elemi matematika köréből.* Typotex Elektronikus Kiadó. Budapest.

- Simon Tamás (szerk.) *Sulinet Digitális Tudásbázis.* Educatio Társadalmi Szolgáltató Kht. Budapest.

- Singh, Simon 2001. *Kódkönyv.* Park Könyvkiadó. Budapest.

- Staar Gyula 2006. Fazekas, ELTE, Microsoft, IMU - Beszélgetés Lovász László akadémikussal *Természet Világa* 11: 484–489.

- T. Dénes Tamás 2004. *TitokTan Trilógia 2. rész Klasszikus RejTények Kriptográfiai ARCképcsarnok.* Bagolyvár Könyvkiadó. Budapest.

- Tarján Tamás. 1917. április 6. - Az Egyesült Államok belép az első világháborúba. *Rubicon Kalendárium.* Rubicon-Ház Bt. Budapest.

- Verne, Jules 1980. *Sándor Mátyás.* Móra Könyvkiadó. Budapest.

- Verne, Jules 1998. *Utazás a Föld középpontja felé.* Unikornis. Budapest.

- Weisstein, Eric W. 2009. 47th Known Mersenne Prime Apparently Discovered. *Wolfram Mathworld.*

7. Mellékletek

7.1. 1. számú melléklet: Témavezetői bírálat

7.2. 2. számú melléklet: A szakdolgozati konzultáció igazolólapja

7.3. 3. számú melléklet: Eredetiságnyilatkozat