Wettl Ferenc

# Varázslók titkai – a nem feltáró bizonyítás

## 1. Varázslók titkai

### 1.1. Történet egy varázslóról

A régi korok nagy titkokat tudó varázslóinak nehéz volt a sorsa: egész életük félelemben telt, rettegtek, hogy kincsként őrzött titkuk kitudódik. A Nagy Zöld Sárkány uralkodásának 125. éve azonban olyasmit hozott, ami megváltoztatta a varázslók életét. Történt pedig, hogy Bebió, a „békából királyfit" varázsigéit olyan szintre fejlesztette, hogy bármilyen állatot szinte bármivé át tudott változtatni. A varázslás történetében először olyan varázsigét használt, ami minden alkalommal más, és más volt, szavai nemcsak az állat fajtájától, de még a nap pillanatnyi állásától is függtek. Egy este például hatalmas nézősereg előtt csak annyit mondott: „beáz nih lókista!", mire a kezében tartott patkány kösöntyűvé vált. Kisvártatva így szólt: „viszka!", s a patkány ismét ott ficánkolt ujjai között. Másnap reggel farkánál fogva lóbált egy hermelint, amiből a közönség kívánságára tepsi lett, amint kimondta a „röcsi hánya távé!" szavakat. A visszavarázsláshoz – mint mindig – most is elég volt csak annyit mondania: „viszka!".

Reménytelennek tűnt, hogy akad aki megfejti e titkot. Voltak, akik nem is hittek Bebiónak, csalást szimatoltak. Azt sejtették, hogy Bebio csak a saját, varázsszerekkel előre preparált állataival mesterkedik. Ellea, a kétkedéséről ismert híres boszorka ravasz tervet eszelt ki. Sokak jelenlétében meghívta Bebiót saját tanyájára, hogy a következő hét minden napján napkeltekor, és napnyugtakor változtassa át azokat az állatokat, amiket ő tesz elé, s azzá, amit ő akkor kitalál. „Elhiszem, hogy nem olcsó bűvészmutatvány az egész, ha ezt az egyhetes próbát kiállod!" – mondta. Bebió kényszeredett mosolya jelezte, nehezen tud mit válaszolni. Ha visszautasítja a kérést, azt fogják gondolni, hogy csalás van a dologban. Ha elfogadja a meghívást, akkor arra számíthat, hogy gondosan megtervezett kísérletekben kell részt vennie, például ugyanazokat az állatokat kell majd többször hasonló körülmények között átváltoztatnia, így Ellea megtudhat valamit titkaiból. Bebió csapdába esett, nemigen mond-

hatott nemet, ha viszont igent mond, féltve őrzött titkai kerülhetnek veszélybe. Reménykedve, hogy a hátralévő napok alatt lesz még valami mentő ötlete, végül elfogadta a meghívást.

Bebió látta, a csapdából csak úgy mászhat ki, ha meg tudja győzni Elleát arról, hogy tudja a bármilyen állatból bármit varázslás titkát, de ezt nem az Ellea által előkészített állatokkal teszi. Sok töprengés után Bebió kitalált valami furfangosat. A következő ötlettel kereste fel Elleát:

– Ellea! Arra gondoltam, hogy amikor majd elém raksz egy állatot, én átmegyek vele egy másik szobába, ahol senki sem láthat, ott átváltoztatom a te állatodat valamilyen másik állattá. Ezután visszajövök, és ezt az állatot azzá változtatom, amivé te csak akarod. Így majd láthatod a varázslatot, de nekem sem kell félnem attól, hogy kifürkészel valamit a titkomból. – Nem, nem! – válaszolta Ellea. – Lehet, hogy te csak a saját preparált állataiddal tudod a „varázslatot". A másik szobában eltünteted az enyémet, és a tiéddel jössz vissza! Ez így nem varázslat, csak olcsó, gyerekeknek való régi trükk! Rotulfo Varázsdoboz I-ében van is egy ilyen játék fehér egér. – Számítottam erre az ellenvetésre. Arra gondoltam, ha visszajövök az állattal, két lehetőséget kínálok fel neked. Egyik esetben arra kérhetsz, hogy a „viszka!" varázsszóval változtassam vissza az állatodat. Ha ezt választod, azonnal ellenőrizheted, hogy az állat valóban a tiéd-e, nem cseréltem-e ki a sajátomra. A másik lehetőséged az lenne, hogy megmondod mivé változtassam az állatot. Így meg azt ellenőrizheted, hogy tudom-e a varázslatot. Tehát ha én a saját állatommal állok eléd, te pedig azt kéred tőlem, varázsoljam vissza, le fogok bukni, ha pedig a te átváltoztatott állatoddal jövök vissza, de nem tudom a varázslatot, akkor nem leszek képes átváltoztatni azzá, amit kérsz. Ha rajtakapsz, világgá kürtölheted, hogy hazudtam. – Nem, nem! Nem tetszik. Sosem lehetek biztos abban, hogy nem csak a szerencsén múlott-e az egész. Ha mindig épp akkor hozod a saját állatodat, amikor arra kérlek varázsolj, és pont akkor hozod vissza az enyém, amikor arra kérlek, változtasd vissza, nem fogsz lebukni! – Ez igaz! Ha csak egyszer próbálkozunk, 1/2 az esélye, hogy ez történjen, de ha mondjuk 10-szer, akkor már $1/2^{10}$, azaz $1/1024$. De tőlem próbálkozhatunk 50-szer is. Ha nem tudom a titkot, így már csak $1/1\,125\,899\,906\,842\,624$ az

esélye[1] annak, hogy nem bukom le. Ez a valószínűség már olyan kicsi, hogy még varázslók közt sincs reális esély a bekövetkeztére. – Hmm. Én nem szerencsejátékra hívtalak, azért szerveztem meg ezt a hetet, hogy megtudjak valamit! – Egy hét múlva vagy biztosan tudni fogod, hogy én csaló vagyok, vagy elegendően nagy biztonsággal azt, hogy valóban tudom a titkot! Gondolom a barátaid, sőt az ellenségeid is jelezték már, hogy tanui szeretnének lenni annak, ami a történni fog nálad a jövő héten. Ha valami kiderül a titkaimból azt ők is megtudják, s így hamar tudni fogja mindenki. Ha viszont úgy járunk el, ahogy javasoltam, te meggyőződhetsz róla, hogy tudom a titkot, ők viszont még ezt sem tudják meg. Azt hihetik, hogy összebeszéltünk, és te mindig épp azt kéred tőlem, amiben előre megállapodtunk. Amit látnak, nekik semmit sem fog bizonyítani! Meg fogja őket ütni a guta!

Ez az érv végre hatott, s a következő héten *Bebi*ó *bebi*zonyította Elleának, hogy valóban tudja a titkot, *Elle*a pedig *elle*nőrizhette mindezt, s a bizonyítást elfogadta, amint a bizonyossághoz számára is elegendően közel értek! És ami Bebiónak olyan fontos volt: titkaiból sem Ellea, sem vendégei nem tudtak meg semmi használhatót.

Bebió e módszerének különféle változatait a varázslók azóta is használják, ha egy varázstitok ismeretét akarják úgy bizonyítani, hogy közben a lehető legkevesebbet tárják fel tudásukból. Az ilyen bizonyítást *legkevésbé feltáró* bizonyításnak nevezik. Ha a bizonyítás olyan, hogy abból egyáltalán semmi sem derülhet ki a titokról, akkor *nem feltáró bizonyítás*ról[2] beszélünk.

Bár közvetlenül nem vág írásunk témájába, megemlítjük a történet folytatását is. Ellea a következő hónapokban többször is meghívta tanyájára Bebiót hasonló nyilvános bemutatókra. Hamarosan elterjedt a pletyka, hogy Ellea összejátszik Bebióval. Ellea ugyan határozottan tagadta a vádat, de olyan megfejthetetlen mosoly kísérte szavait, ami jót tett a pletyka terjedésének. Aztán másfél év múlva Ellea feleségül ment Bebióhoz, ő pedig megosztotta titkait hitvesével.

---

[1] Bebió fiatal korában a nagy számok mágiájával foglalkozott, innen e varázslók közt ritka fejszámoló képessége.

[2] Angol nyelvterületről származó varázslók leggyakrabban a „zero knowledge proof" kifejezést használják e módszerre.

### 1.2. Mit tanulhatunk a varázslóktól?

Titkaink nekünk hétköznapi embereknek is vannak, köztük olyanok is, melyek tudását nap mint nap bizonyítanunk kell. Gondoljunk csak a bankkártyára. Ahhoz, hogy pénzhez jussunk, be kell bizonyítanunk, hogy ismerjük a kártya pin-kódját. A módszer, amit jelenleg használunk, a lehető legprimitívebb. Kiadjuk teljes titkunkat, abban bízva, hogy a gépen keresztül senki nem fog hozzájutni. Jelenleg a legtöbb helyen ugyanez játszódik le egy központi számítógépre való belépéskor is. Begépeljük a saját azonosítónkat, majd saját jelszavunkat, amit a hálózaton, vagy a gépben számtalan módon el lehet lopni (mi pedig nyugodtak vagyunk, mert jelszavunkat nem látjuk kiíródni a képernyőre).

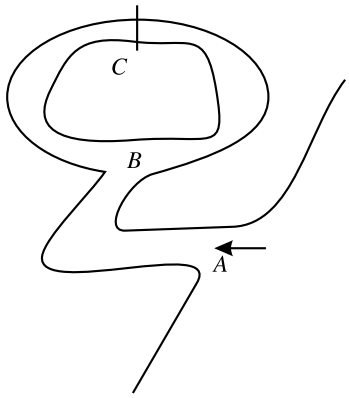
E dolgozat témája a kriptográfiának, azaz a titkosítás tudományának a nem feltáró bizonyításról szóló fejezete, mely az 1980-as évek közepén született. E téma tanulmányozása a matematika több területének elemi ismeretét igényli, ezek közül a legfontosabbak a számelmélet, az algoritmusok bonyolultságának elmélete és a valószínűségszámítás. Ennyi mindent e bevezető ismertetőben nem tudunk áttekinteni, ezért csak egy területre, a számelméletre koncentrálunk. Szükségünk lesz a számítási bonyolultság fogalmára. Erről bővebben esik szó Lovász László e könyvben megjelent cikke első részében. Azt fogjuk mondani, hogy egy számítási feladat hatékonyan vagy gyorsan elvégezhető, ha van olyan eljárás a feladat megoldására, melynek végrehajtásához szükséges idő bármely input esetén az input méretét jellemző számnak valamely polinomjával (például négyzetével) becsülhető. Ha egy számítási feladat megoldásához szükséges idő az input méretét jellemző szám exponenciális függvénye, akkor a számítási feladatot bonyolultnak fogjuk tekinteni. A továbbiakban ismertetendő titkosítási eljárások azon alapulnak, hogy egy konkrét számítási feladat jelen tudásunk szerint bonyolult (megoldása a gyakorlatban évszázadokig tartana a mai leggyorsabb számítógépekkel), míg valami további információ felhasználásával hatékonyan kiszámíthatóvá válik (a gyakorlatban pl. a másodperc törtrésze alatt).

A kriptográfia irodalmából csak két alapvető munkára, az [4] és [7] könyvekre hivatkozunk, melyek számtalan további hivatkozást tartalmaznak. Közülük az [4] könyv e mű írásakor az interneten legálisan és ingyen is elérhető. A magyar nyelvű kriptográfiai témájú könyvek közül kettőt említünk, Ködmön József [3] mun-

kája az informatikai biztonság alapjaival és a PGP nevű titkosító rendszer használatával foglalkozik, míg Singh Kódkönyve a kriptográfia történetéről ad áttekintést [6].

E fejezet befejezéseként egy egyszerű, a kriptográfia népszerűsítő irodalmából ismert, matematikán kívüli nem feltáró bizonyítás megkonstruálását kérjük az Olvasótól.

*1. feladat.* A mellékelt térképen egy barlang járatai láthatóak. Az $A$ pontnál van a barlang bejárata, $B$-nél egy elágazás, a két út $C$-nél egy körbe zárul, ahol egy kapu van. Az $A$ pontból nem látszik $B$, és sem $A$-ból, sem $B$-ből nem látszik $C$. Bianka tudja a kapu kinyitásának titkos módját, Elemér nem. Hogyan bizonyíthatja Bianka Elemérnek, hogy ki tudja nyitni a kaput, ha nem akarja, hogy Elemér meglássa a kapu kinyitását. Mit tegyenek, ha ugyanakkor Elemér nem szeretné, ha a folyton nyomában járó, s minden lépését figyelő Fidél is meggyőződhetne arról, hogy Bianka tudja a titkot?




## 2. Számolás maradékokkal

A továbbiakban szükségünk lesz a számelmélet néhány alapfogalmára. Először a moduláris összeadás és szorzás, a moduláris inverz, majd a moduláris négyzetgyökvonás fogalmával és néhány alaptulajdonságával ismerkedünk meg. Közben szükségünk lesz a kínai maradéktétel egy speciális esetére is. E fejezetet átugorhatja a

számelmélet elemi alapfogalmaiban járatos olvasó. A számelmélettel való ismerkedéshez Sárközi András művét [5] valamint Szalay Mihálynak a Speciális Matematika Tankönyvek sorozatban megjelent könyvét [8] ajánljuk. További tanulmányokhoz Freud Róbert és Gyarmati Edit egyetemi tankönyve javasolható [2], de az érdeklődő több érdekes és olvasásra érdemes számelméleti témájú könyvet talál az elmúlt évtizedekben magyarul megjelent könyvek között.

### 2.1. Moduláris összeadás és szorzás

Ismeretes, hogy a maradékos osztás egész számok között egyértelműen elvégezhető, azaz, ha $a$ és $m$ egész számok és $m > 0$, akkor egyetlen olyan $q$ és $r$ egész létezik, hogy $a = mq + r$ és $0 \leq \leq r < m$. Az $r$ számot az $a$ szám $m$-mel való osztási *maradék*ának nevezzük. Azt is szokás mondani a fenti $r$ maradékra, hogy az „$a$ maradéka modulo $m$". E maradékra az $a \bmod m$ jelölést használjuk. Itt tehát mod egy kétváltozós művelet jele. Példaként legyen $a = 17$ és $m = 5$. Ekkor $17 = 5 \cdot 3 + 2$, tehát $q = 3$ és $r = 2$, azaz $17 \bmod 5 = 2$.

Ha $a$ és $b$ az $m$-mel osztva azonos maradékot ad, akkor azt mondjuk, hogy $a$ *kongruens* $b$*-vel modulo* $m$, és ezt úgy jelöljük, hogy $a \equiv b \pmod{m}$. Például $11 \equiv 47 \pmod{9}$, mert 9-cel osztva 11, és 47 is 2-t ad maradékul. Ne keverjük össze a két „mod" jelölést: $a \equiv b \pmod{m}$ azzal ekvivalens, hogy $a \bmod m = b \bmod m$. Az előbbi példánkban $11 \bmod 9 = 2$ és $47 \bmod 9 = 2$, tehát valóban $11 \equiv 47 \pmod{9}$.

Könnyen látható, hogy $a \equiv b \pmod{m}$ pontosan akkor teljesül, ha $m$ osztója $b - a$-nak. E tulajdonság felhasználásával igazolható, hogy ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$ és $ac \equiv bd \pmod{m}$. Például $a \equiv 1 \pmod{2}$, $b \equiv 0 \pmod{2}$ esetén $a + b \equiv 1 \pmod{2}$ és $ab \equiv 0 \pmod{2}$, ami egyébként azzal ekvivalens, hogy egy páros és egy páratlan szám összege páratlan, míg szorzata páros.

Az előzőekből azonnal adódik, hogy ha egy egészekből álló kifejezésben csak az összeadás, kivonás és szorzás művelete szerepel, akkor e kifejezés értékének modulo $m$ vett maradéka nem fog megváltozni, ha benne bármelyik számot kicseréljük egy vele modulo $m$ kongruens számmal. Például $(-5 + 12)(-6 + 10) \equiv (4 - 6)(12 - 8) \pmod{9}$, mivel $-5 \equiv 4 \pmod{9}$, $12 \equiv -6 \pmod{9}$ és $10 \equiv -8 \pmod{9}$. Ez

vezet a maradékosztályokkal való számolás, más néven a *moduláris aritmetika* fogalmához.

Az egész számok osztályokba sorolhatók úgy, hogy egy osztályba kerüljenek azok a számok, amelyek egy rögzített pozitív egész $m$ számmal osztva azonos maradékot adnak. Jelölje $[k]_m$ vagy egyszerűen csak $[k]$ azt az osztályt, melynek minden eleme $k$ maradékot ad. Például modulo 3 a következő három maradékosztály létezik: $[0]_3 = \{\ldots, -3, 0, 3, 6, \ldots\}$, $[1]_3 = \{\ldots, -2, 1, 4, 7, \ldots\}$, $[2]_3 = \{\ldots, -1, 2, 5, 8, \ldots\}$. Miután az, hogy a fenti három művelettel elvégzett számolás eredménye melyik osztályba esik csak attól függ, hogy mely osztályba eső számmal számoltunk, természetes módon definiálhatjuk a maradékosztályok közti műveleteket. $[a]_m + [b]_m = [c]_m$, illetve $[a]_m[b]_m = [d]_m$, ha egy $[a]_m$ és egy $[b]_m$ osztályból vett szám összege a $[c]_m$, illetve szorzata a $[d]_m$ osztályba esik. Például $[2]_3 + [1]_3 = [0]_3$ és $[2]_3[1]_3 = [2]_3$, mert például $4 + 2 = 6$ és $4 \cdot 2 = 8$. Azt a struktúrát, amit a modulo $m$ maradékosztályok a köztük definiált fenti műveletekkel alkotnak $\mathbb{Z}_m$-mel jelöljük. Például $\mathbb{Z}_3$ elemei $\{[0]_3, [1]_3, [2]_3\}$, míg az elemek közt definiált két művelet táblája:

| + | $[0]_3$ | $[1]_3$ | $[2]_3$ |
|---|---|---|---|
| $[0]_3$ | $[0]_3$ | $[1]_3$ | $[2]_3$ |
| $[1]_3$ | $[1]_3$ | $[2]_3$ | $[0]_3$ |
| $[2]_3$ | $[2]_3$ | $[0]_3$ | $[1]_3$ |

| × | $[0]_3$ | $[1]_3$ | $[2]_3$ |
|---|---|---|---|
| $[0]_3$ | $[0]_3$ | $[0]_3$ | $[0]_3$ |
| $[1]_3$ | $[0]_3$ | $[1]_3$ | $[2]_3$ |
| $[2]_3$ | $[0]_3$ | $[2]_3$ | $[1]_3$ |

Könnyen látható, hogy ha $a$ és $m$ relatív prímek, azaz $a$ és $m$ legnagyobb közös osztója 1, akkor $[a]_m$ minden eleme relatív prím $m$-hez. Ha két modulo $m$ maradékosztály ilyen tulajdonságú, akkor a szorzatuk is.

Az olyan maradékosztályoknak, melyek elemei relatív prímek $m$-hez, a szorzás műveletével alkotott struktúráját $\mathbb{Z}_m^*$-gal jelöljük. Például $\mathbb{Z}_{12}^*$ elemei: $[1]_{12}$, $[5]_{12}$, $[7]_{12}$, $[11]_{12}$; művelettáblája:

| × | $[1]_{12}$ | $[5]_{12}$ | $[7]_{12}$ | $[11]_{12}$ |
|---|---|---|---|---|
| $[1]_{12}$ | $[1]_{12}$ | $[5]_{12}$ | $[7]_{12}$ | $[11]_{12}$ |
| $[5]_{12}$ | $[5]_{12}$ | $[1]_{12}$ | $[11]_{12}$ | $[7]_{12}$ |
| $[7]_{12}$ | $[7]_{12}$ | $[11]_{12}$ | $[1]_{12}$ | $[5]_{12}$ |
| $[11]_{12}$ | $[11]_{12}$ | $[7]_{12}$ | $[5]_{12}$ | $[1]_{12}$ |

A továbbiakban az egyszerűség kedvéért $\mathbb{Z}_m$ és $\mathbb{Z}_m^*$ elemeit a szögletes zárójeleket elhagyva, a maradékosztályból választott valamely

reprezentánssal fogjuk jelölni. E reprezentánsokat leggyakrabban a $\{0, 1, \ldots, m-1\}$ halmazból választjuk. Tehát e megállapodás után $\mathbb{Z}_{12}^*$ elemeinek halmaza $\{1, 5, 7, 11\}$, ha pedig $m$ prím, akkor $\mathbb{Z}_m^*$ elemeinek halmaza $\{1, 2, \ldots, m-1\}$. A $-1$ mint $\mathbb{Z}_m$ egy eleme, ugyanazt jelöli, mint $m-1$. Ha $m = 1$, akkor $\mathbb{Z}_m$-nek csak egy eleme van, $\mathbb{Z}_m^*$ pedig nem is létezik, ezért a továbbiakban feltesszük, hogy $m > 1$.

### 2.2. Moduláris inverz

Könnyen megmutatható, hogy $\mathbb{Z}_m^*$ elemeit beszorozva egy $a \in \mathbb{Z}_m^*$ elemmel, $\mathbb{Z}_m^*$ elemeinek egy permutációját kapjuk, amit másként úgy is kifejezhetünk, hogy az $a \cdot x = b$ egyenlet minden $a, b \in \mathbb{Z}_m^*$ esetén egyértelműen megoldható (az $a$ és $x$ közti szorzásjel a $\mathbb{Z}_m^*$-beli művelet jelöli!). Speciálisan $b = 1$ esetén azt kapjuk, hogy minden $a \in \mathbb{Z}_m^*$ maradékosztályhoz található egyetlen olyan $\bar{a} \in \mathbb{Z}_m^*$ maradékosztály, melyre $a \cdot \bar{a} = 1$. Ezt a maradékosztályt nevezzük az $a$ maradékosztály *inverz*ének. Az $a \in \mathbb{Z}$ egész *moduláris inverz*én az $a$-val reprezentált maradékosztály $\bar{a}$ inverzének 0 és $m$ közé eső reprezentánsát értjük, és erre az elemre az $a^{-1} \bmod m$ jelölést használjuk.

A moduláris inverz létezése a kongruenciák nyelvén így fogalmazható meg: az $ax \equiv 1 \pmod{m}$ kongruencia minden $m > 1$ egész és minden $m$-hez relatív prím $a \in \mathbb{Z}$ esetén egyértelműen megoldható, azaz egyetlen olyan $a' \in \mathbb{Z}$, $0 < a' < m$ egész létezik, hogy a fenti kongruenciát kielégítő $x$ számok pontosan azok, melyek eleget tesznek az $x \equiv a' \pmod{m}$ kongruenciának.

Lássunk két példát: $\mathbb{Z}_7^*$-ban $\bar{1} = 1$, $\bar{2} = 4$, $\bar{3} = 5$ és $\bar{6} = 6$, míg a fenti művelettáblán könnyen ellenőrizhető, hogy $\mathbb{Z}_{12}^*$ minden eleme saját maga moduláris inverze, azaz $a \in \mathbb{Z}_{12}^*$ esetén $a^{-1} \bmod 12 = a$.

Kérdés, hogy miként számítható ki minél gyorsabban a moduláris inverz. A következőkben az euklideszi algoritmus egy erre a feladatra kihegyezett változatát fogjuk ismertetni. Kezdjük egy egyszerű példával. Számítsuk ki $5^{-1} \bmod 13$ értékét! A részeredményeket egy kétoszlopos táblázatban fogjuk feljegyezni, melynek első sorában $m$ és 0, míg második sorában $a$ és 1 áll:

| $m$ | 0 | | | 13 | 0 |
|---|---|---|---|---|---|
| $a$ | 1, | azaz esetünkben | | 5 | 1 |

Ezután a táblázat további sorait rekurzív módon a megelőző kettőből a következő egyszerű képlettel fogjuk kiszámítani:[3]

| | |
|---|---|
| $y_1$ | $x_1$ |
| $y_2$ | $x_2$ |
| $y_1 - \lfloor \frac{y_1}{y_2} \rfloor y_2$ | $x_1 - \lfloor \frac{y_1}{y_2} \rfloor x_2$ |

Ezt az eljárást addig ismételjük, amíg a bal oldalon 1-et nem kapunk. Ekkor a jobb oldalon $a$ inverze fog állni, egészen pontosan az inverz maradékosztály egy eleme. Az $m = 13$, $a = 5$ értékekkel számolva a következő táblázatot kapjuk (a második oszlop mellett zárójelben megadjuk a részletszámításhoz használt $\lfloor \frac{y_1}{y_2} \rfloor$ értékeket is):

| | | |
|---|---|---|
| 13 | 0 | |
| 5 | 1 | $(\lfloor \frac{13}{5} \rfloor = 2)$ |
| 3 | $-2$ | $(\lfloor \frac{5}{3} \rfloor = 1)$ |
| 2 | 3 | $(\lfloor \frac{3}{2} \rfloor = 1)$ |
| 1 | $-5$ | |

Azt kaptuk tehát, hogy az 5-tel reprezentált $\mathbb{Z}_{13}$-beli mellékosztály inverze a $-5$-tel reprezentált maradékosztály, de mivel $-5 \equiv 8 \pmod{13}$, ezért ez megegyezik a $8 \in \mathbb{Z}_{13}$ mellékosztállyal. Összefoglalva tehát: $5^{-1} \bmod 13 = 8$.

Annak bebizonyításához, hogy ha $m$ és $a$ relatív prímek ($m > a$), akkor a fenti eljárással megkapjuk $a^{-1} \bmod m$ értékét, két állítást kell igazolni:

1. A bal oldali oszlopban véges sok lépésen belül eljutunk az 1-eshez.
2. A táblázat mindegyik sorának bal oszlopában álló $y$ és jobb oszlopában álló $x$ számok teljesítik az $ax \equiv y \pmod{m}$ feltételt, így az utolsó sorban álló $x$ számra $ax \equiv 1 \pmod{m}$.

[3] Az $\lfloor x \rfloor$ az $x$ valós szám *egész részét* jelöli, azaz azt a legnagyobb egészt, mely nem nagyobb $x$-nél. Például $\lfloor \frac{4}{3} \rfloor = 1$, $\lfloor -\pi \rfloor = -4$. Ha $m > 0$ és $a$ egészek, akkor a maradékos osztás szerinti $a = mq + r$ ($0 \leq r < m$) összefüggésben szereplő $q$ és $r$ kifejezhető e függvény segítségével: $q = \lfloor \frac{a}{m} \rfloor$, $r = a - \lfloor \frac{a}{m} \rfloor m$.

Az első állítás bizonyításához elég megmutatni, hogy az egymás után következő számok mindig relatív prímek, továbbá hogy szigorúan monoton csökkenő sorozatot alkotnak. A második állítás nyilvánvalóan igaz a táblázat első két sorára, a továbbiakra pedig a kongruenciák korábban említett tulajdonságaiból levezethető. A bizonyítások kidolgozását az olvasóra bízzuk.

Még meglehetősen nagy számok esetén is gyorsan számolható a moduláris inverz. A következő feladat számítógép használata nélkül is gyorsan megoldható.

*2. feladat.* Határozzuk meg $242424242^{-1} \bmod 12121212121$ értékét! (A két adott szám relatív prím, mivel 12121212121 prím.)

### 2.3. Kínai maradéktétel

A kínai maradéktétel lineáris kongruenciarendszerek megoldhatóságáról szól. Nekünk csak egy speciális esetére lesz szükségünk. Legyen $p$ és $q$ két különböző prím, és $a, b \in \mathbb{Z}$ tetszőleges egészek. Ekkor az

$$x \equiv a \pmod{p}$$
$$x \equiv b \pmod{q}$$

kongruenciarendszer megoldható, és a megoldás egyértelmű modulo $pq$. A megoldás egyszerűen meg is konstruálható. Jelölje $\bar{p}_q$ a $p$ inverzét mod $q$, míg $\bar{q}_p$ a $q$ inverzét mod $p$, azaz legyenek igazak a $q\bar{q}_p \equiv 1 \pmod{p}$ és $p\bar{p}_q \equiv 1 \pmod{q}$ kongruenciák. Nagyon könnyű ellenőrizni, hogy ekkor az $x = aq\bar{q}_p + bp\bar{p}_q$ megoldása a fenti kongruenciarendszernek. Az egyértelműség bizonyításához csak azt kell megmutatni, hogy bármely két megoldás különbsége osztható $pq$-val. Ezek igazolását az olvasóra bízzuk.

*3. feladat.* Oldjuk meg az

$$\begin{aligned} x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{11} \end{aligned} \quad \text{és az} \quad \begin{aligned} x &\equiv -2 \pmod{7} \\ x &\equiv -3 \pmod{11} \end{aligned}$$

kongruenciarendszereket!

### 2.4. Moduláris hatványozás és négyzetgyökvonás

Egy szám moduláris négyzetreemelése nem jelent újat, hisz ez csak egy moduláris szorzás. Segítségével a moduláris hatványozás

is gyorsan elvégezhető. A módszer lényege, hogy a részletszámításokat is modulárisan végezzük, így mindig kisebb számokkal kell számolnunk, másrészt ismételt négyzetreemelésekkel kiszámítjuk az alap kettőhatvány-kitevőjű hatványait, amelyek közül a megfelelőek összeszorzásával megkapjuk az eredményt. További magyarázat helyett csak egy egyszerű példát mutatunk.

Számítsuk ki $9^{22} \mod 79$ értékét számológép használata nélkül! Először ismételt négyzetreemelésekkel kiszámítjuk 9 kettőhatvány-kitevőjű hatványait: $9^2 = 81 \equiv 2 \pmod{79}$, $9^4 = (9^2)^2 \equiv 2^2 \equiv 4 \pmod{79}$, $9^8 = (9^4)^2 \equiv 4^2 \equiv 16 \pmod{79}$, $9^{16} = (9^8)^2 \equiv 16^2 = 256 \equiv 19 \pmod{79}$. Ezután a kitevőt, azaz 22-t felbontjuk kettőhatványok összegére (ez a kitevő kettes számrendszerbeli alakjának felírásával ekvivalens feladat): $22 = 16+4+2$ (a 22 kettes számrendszerbeli alakja 10110). Így $9^{22} = 9^{16} \cdot 9^4 \cdot 9^2 \equiv 19 \cdot 4 \cdot 2 \equiv 73 \pmod{79}$, tehát $9^{22} \equiv 73 \pmod{79}$.

A négyzetgyökvonás elvégzése általában már korántsem ilyen egyszerű feladat. Mielőtt ennek vizsgálatára térnénk, felelevenítünk egy definíciót és két fontos számelméleti alaptételt:

Legyen $n$ pozitív egész, és legyen $(a, n) = 1$. Azt mondjuk, hogy az $a$ szám *négyzetelem* modulo $n$, ha van olyan $x$ egész, hogy $x^2 \equiv a \pmod{n}$.

- *kis Fermat-tétel:* Ha $p$ prím és $a$ nem osztható $p$-vel, akkor

$$a^{p-1} \equiv 1 \pmod{p}.$$

- *Euler-feltétel:* Ha $p > 2$ prím és $a$ nem osztható $p$-vel, akkor az $x^2 \equiv a \pmod{p}$ kongruencia pontosan akkor oldható meg – azaz $a$ pontosan akkor *négyzetelem* modulo $p$ –, ha

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

  és ekkor a fenti kongruenciának modulo $p$ két különböző megoldása van. Ha az egyik megoldás $x_0$, akkor a másik $-x_0$ (ha a gyökök 0 és $p$ közé eső reprezentánsait keressük, tehát $0 < x_0 < p$, akkor a másik megoldás reprezentánsa $p - x_0$).

Az utóbbi tétel felhasználásával könnyen bizonyítható, hogy abban az esetben, ha $p$ $4k + 3$ alakú prím és $a$ négyzetelem, akkor $a$ két négyzetgyöke

$$\pm a^{\frac{p+1}{4}},$$

ugyanis $(\pm a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} a \equiv a \pmod{p}$.

*4. feladat.* Határozzuk meg 2 és 5 négyzetgyökeit modulo 31.

Ha a modulus nem prím, de két $4k + 3$ alakú prím szorzata, akkor e prímtényezők ismeretében könnyen kiszámítható bármely négyzetelem négyzetgyöke. A két $4k + 3$ alakú prím szorzataként előálló egészeket *Blum-egészek*nek nevezik.

Legyen $n = pq$, ahol $p$ és $q$ két különböző prím, és tegyük fel, hogy az $x^2 \equiv a \pmod{n}$ $(0 < a < n)$ kongruenciának $x_0$ egy megoldása. Először megmutatjuk, hogy e kongruenciának modulo $n$ négy különböző megoldása, azaz $a$-nak négy különböző négyzetgyöke van, ha $a$ és $n$ relatív prímek. Legyen $x_p$, illetve $x_q$ az a két egész szám, melyekre $x_p \equiv x_0 \pmod{p}$ és $0 < x_p < p$, illetve $x_q \equiv x_0 \pmod{q}$ és $0 < x_q < q$. Minthogy $x^2 \equiv a \pmod{n}$ megoldható, ezért $x^2 \equiv a \pmod{p}$ is, és a két gyöke $x_p$ és $-x_p$. Hasonlóképpen $x^2 \equiv a \pmod{q}$ két gyöke $x_q$ és $-x_q$. A kínai maradéktételből következik, hogy az $x^2 \equiv a \pmod{n}$ $((a, n) = 1)$ kongruenciának pontosan négy megoldása van, melyeket a következő négy kongruenciarendszer megoldásából kaphatunk meg:

$$\text{(1)} \quad \begin{aligned} x &\equiv x_p \pmod{p} \\ x &\equiv x_q \pmod{q} \end{aligned} \qquad \text{(2)} \quad \begin{aligned} x &\equiv x_p \pmod{p} \\ x &\equiv -x_q \pmod{q} \end{aligned}$$

$$\text{(3)} \quad \begin{aligned} x &\equiv -x_p \pmod{p} \\ x &\equiv x_q \pmod{q} \end{aligned} \qquad \text{(4)} \quad \begin{aligned} x &\equiv -x_p \pmod{p} \\ x &\equiv -x_q \pmod{q} \end{aligned}$$

Könnyen bizonyítható, hogy a négy különböző gyök közül kiválasztható kettő úgy – jelölje ezeket $x_1$ és $x_2$ –, hogy a négy négyzetgyök kongruens legyen az alábbi négy számmal modulo $n$: $x_1$, $x_2$, $-x_1$, $-x_2$.

Az előbbiekben feltételeztük, hogy már ismerjük az $x^2 \equiv a \pmod{n}$ kongruencia egy megoldását. Ez általában persze nincs így, ha azonban $n$ Blum-egész, azaz $p \equiv q \equiv 3 \pmod{4}$, akkor az $x^2 \equiv a \pmod{p}$, illetve az $x^2 \equiv a \pmod{q}$ kongruenciákat $x_0$ ismerete nélkül is meg tudjuk oldani, így az (1)–(4) kongruen-

ciarendszerek az alábbi alakba írhatóak:

$$(5)\qquad \begin{aligned} x &\equiv \pm a^{\frac{p+1}{4}} \pmod{p} \\ x &\equiv \pm a^{\frac{q+1}{4}} \pmod{q} \end{aligned}$$

*5. feladat.* Határozzuk meg 53-nak modulo 77 vett négyzetgyökeit!

### 2.5. A prímtényezős felbontás és a gyökvonás

A titkosítás tudományának mai módszerei közül igen sok egyrészt arra a sejtésre épül, hogy egy egész szám prímtényezőkre bontása igen számításigényes feladat, másrészt arra a tényre, hogy vannak olyan számítási feladatok, melyek a prímtényezők ismeretében igen gyorsan elvégezhetők, a prímtényezők ismerete nélkül viszont csak legalább olyan nagy munkával, mint maga a prímtényezőkre bontás. Például ha valaki csak annyit tud egy számról, hogy az két 200-jegyű prím szorzata, akkor ismereteink és a számítástechnika mai fejlettsége mellett prímtényezőkre bontásához sok évtizednyi gépidőre lenne szükség a leggyorsabb mai gépeken is. Tetszőleges, $n$-hez relatív prím egész szám négy négyzetgyökének meghatározása a korábban megismert algoritmussal a másodperc tört része alatt elvégezhető még egy egyszerű PC-n is, ugyanakkor a prímtényezők ismerete nélkül is gyorsan lefutó algoritmus nem ismeretes. Az, hogy ilyen algoritmus nem létezik, nincs bizonyítva, azt azonban magunk is ellenőrizhetjük, hogy ha volna, akkor lenne a prímtényezős felbontásra is gyors algoritmus.

Tegyük fel tehát, hogy „gyorsan” ki tudjuk számolni egy $n$-nel relatív prím $a$ szám modulo $n$ vett négy négyzetgyökét. Jelölje a négy gyököt $x_1$, $x_2$, $-x_1$ és $-x_2$, ahol $0 < x_1 < x_2 < n$. Mivel $x_1^2 \equiv x_2^2 \pmod{n}$, azaz $x_2^2 - x_1^2 \equiv 0 \pmod{n}$, de $x_1 \not\equiv \pm x_2 \pmod{n}$, ezért $(x_2 - x_1, n)$ valódi osztója $n$-nek. A legnagyobb közös osztó a prímtényezők ismerete nélkül is gyorsan számolható az euklideszi algoritmussal, ezért $n$ „gyorsan” faktorizálható.

Vajon mi történik, ha csak olyan algoritmust ismerünk, mely egy szám négyzetgyökei közül csak egyet (illetve annak ellentettjével együtt kettőt) képes meghatározni? Vajon ekkor meg tudjuk határozni $n$ prímtényezős felbontását? Erre az esetre nagyon egyszerű véletlen algoritmus van. Erről szól a következő feladat.

*6. feladat.* Legyen $n = pq$, és tegyük fel, hogy ismerünk egy olyan $f$ eljárást, mely tetszőleges $a \in \mathbb{Z}_n^*$ elemhez megadja ennek egy $f(a)$ négyzetgyökét. Konstruáljunk olyan véletlen algoritmust, mely 1-hez tetszőlegesen közeli valószínűséggel meghatározza valamely $a$ szám összes gyökét, s ezzel lehetővé teszi $n$ gyors tényezőkre bontását!

Megemlítünk egy másik problémát is, mely a prímtényezők ismeretében könnyen megoldható, ellenkező esetben azonban nem ismeretes gyors algoritmus az eldöntésére. Ez az ún. *négyzetes maradék probléma*, mely a következőképpen szól. Tegyük fel, hogy $n = pq$ két prím szorzata, és jelölje $Q$ azon $m \in \mathbb{Z}_n^*$ egészek halmazát, melyekre az $x^2 \equiv m \pmod{p}$ és a $x^2 \equiv m \pmod{q}$ kongruenciák közül vagy mindkettő megoldható, vagy egyik sem! Másként fogalmazva az $m$ vagy a $\mathbb{Z}_p$-ben és a $\mathbb{Z}_q$-ban is négyzetelem, vagy egyikben sem. Talán meglepő, de az, hogy $m$ eleme-e $Q$-nak, vagy nem, könnyen és igen gyorsan eldönthető akkor is, ha nem ismerjük $p$ és $q$ értékét[4]. Ezek után a kérdés az, hogy egy $m \in Q$ elemről hogyan dönthető el, hogy négyzetelem-e $\mathbb{Z}_n$-ben? Tudjuk, hogy $m \in Q$ pontosan akkor négyzetelem $\mathbb{Z}_n$-ben, ha négyzetelem $\mathbb{Z}_p$-ben és a $\mathbb{Z}_q$-ban is, azaz ha mindkét kongruencia megoldható. Prím modulus esetén az Euler-feltétellel könnyen eldönthető, hogy egy szám négyzetelem-e vagy sem, így ha ismerjük $n$ prímtényezőit, a kérdést gyorsan meg tudjuk válaszolni. Nem ismeretes olyan módszer azonban, melynek segítségével ez a kérdés a prímtényezők ismerete nélkül is gyorsan megválaszolható volna.

Minthogy az $m \in Q$ számokról nehéz eldönteni, hogy négyzetelemek-e vagy sem, ezért az $m \in Q$ elemet *álnégyzet*nek, vagy *álnégyzetelem*nek nevezzük, ha nem négyzetelem.

*7. feladat.* Döntsük el, hogy 19 négyzetelem, álnégyzetelem vagy egyik sem modulo 77. Számítógépet használva soroljuk fel $\mathbb{Z}_{77}^*$ elemei közül az összes négyzetelemet és az összes álnégyzetelemet.

[4] E téma részletesebb taglalására e cikk keretei között nincs módunk, csak annyit jegyzünk meg, hogy ha az $\left(\frac{m}{n}\right)$-nel jelölt ún. Jacobi-szimbólum értéke 1, akkor $m \in Q$, ha $-1$, akkor $m \notin Q$. Definíció szerint $\left(\frac{m}{n}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{q}\right)$, ahol $\left(\frac{m}{p}\right)$ értéke 1 vagy $-1$ aszerint, hogy $m$ négyzetelem vagy nem modulo $p$. Bár a definícióban szerepelnek $n$ prímtényezői, a Jacobi-szimbólum kiszámításához nincs szükség ismeretükre.

# 3. A nem feltáró bizonyítás

## 3.1. A tudás bizonyítása

Legyen $n$ két – legalább százjegyű – prímszám szorzata. Tegyük fel, hogy Bianka ismeri $n$ két prímtényezőjét. Hogyan tudná e tudását bizonyítani Elemérnek anélkül, hogy a két prímet elárulná? Az előző fejezetben mondottak szerint jó bizonyítás lenne, ha egy véletlenül választott $y$ számból rövid időn belül négyzetgyököt tudna vonni modulo $n$. Feltesszük, hogy $(y, n) = 1$, azaz feltesszük, hogy a véletlen $y$ elemet $\mathbb{Z}_n^*$-ból választjuk. Ha $(y, n) > 1$ volna, aminek igen kicsi a valószínűsége, akkor $n$-nek azonnal ismernénk egy prímtényezőjét, és a kérdés érdektelenné válna. Kérdés, hogy Bianka az $y$ négy gyöke közül melyiket adja meg Elemérnek válaszul. Mind a négyet nem adhatja meg, hisz ezek ismeretében Elemér is hamar meg tudná határozni $n$ prímtényezőit. Olyan $T$ tulajdonságot kell tehát találni, melyet mindig pontosan egy gyök elégít ki a négy közül és amelyet Elemér is könnyen tud ellenőrizni. Elemér tehát választ egy $T$ tulajdonsággal rendelkező számot, a négyzetét elküldi Biankának, aki kiszámítja a gyökeit, és kiválasztja közülük az egyetlen $T$ tulajdonsággal rendelkezőt, amit bizonyságul visszaküld Elemérnek.

Megmutatjuk, hogy ha $n$ Blum-egész, azaz $n = pq$, $p$ és $q$ prímek, $p \equiv q \equiv 3 \pmod 4$, akkor egy $n$-nel relatív prím $y$ négyzetelem négy modulo $n$ vett négyzetgyöke között pontosan egy négyzetelem van. A bizonyítás előtt oldjuk meg az alábbi feladatot!

*8. feladat.* A *4.* feladatban kiszámoltuk 53 négyzetgyökeit modulo 77. A négy gyök közül melyik négyzetelem?

Ha $x_0$ a négy négyzetgyök egyike és négyzetelem, azaz az $x^2 \equiv x_0 \pmod n$ kongruenciának van megoldása, akkor van az $x^2 \equiv x_0 \pmod p$ és az $x^2 \equiv x_0 \pmod q$ kongruenciáknak is, azaz, az (1)–(4) kongruenciarendszerekben is használt jelölésekkel, $x^2 \equiv x_p \pmod p$ és $x^2 \equiv x_q \pmod q$ megoldható. Eszerint tehát $x_p$ modulo $p$, míg $x_q$ modulo $q$ négyzetelem. Minthogy $p$ és $q$ 3-mal kongruensek modulo 4, ezért az Euler-feltételből azt kapjuk, hogy $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{q-1}{2}} = -1$, tehát $-1$ nem négyzetelem. Mivel egy négyzet és egy nem négyzet szorzata nem négyzet, így $-x_p$, illetve $-x_q$ sem négyzetelem. Azt kaptuk tehát, hogy az (1)–(4)

kongruenciarendszerek közül pontosan egy van, melynek megoldása négyzetelem.

*9. feladat.* Mutassuk meg, hogy ha $n = pq$ Blum-egész, és $S$ jelöli a modulo $n$ vett négyzetelemek halmazát, akkor az $f: a \in S \mapsto a^2 \bmod n$ függvény $S$ egy permutációját adja, melynek inverze:

$$a \in S \mapsto a^{\frac{(p-1)(q-1)+4}{8}} \bmod n.$$

Ahhoz, hogy a tudás bizonyítására kigondolt algoritmusunk teljes legyen, már csak azt kell biztosítanunk, hogy Elemér egy véletlen négyzetelemet válasszon, és annak négyzetét küldje gyökvonásra Biankának. A legegyszerűbb módszer az, ha Elemér választ egy véletlen $v$ egészt ($0 < v < n$, $(v, n) = 1$), és $v^4$-t küldi Biankának, míg $v^2$-t titokban tartja, hisz épp ez lesz a $v^4$ négyzetgyökei közül a négyzetelem. Így tehát a tudás bizonyítására kitalált protokollunk, a tudását bizonyító Bianka és az azt ellenőrző Elemér részvételével zajló alábbi lépésekből áll:

*1. lépés:* Elemér választ egy véletlen $v \in \mathbb{Z}_n^*$ számot, kiszámolja $y = v^2 \bmod n$ és $z = v^4 \bmod n$ értékét és $z$-t elküldi Biankának, míg $y$-t titokban tartja.

*2. lépés:* Bianka kiszámítja $z$ négyzetgyökeit modulo $n$ és kiválasztja közülük azt a $w$ számot, amelyik négyzetelem (vagy egyszerűen alkalmazza a *9.* feladatbeli képletet), és ezt visszaküldi Elemérnek.

*3. lépés:* Elemér a kapott $w$ számot összeveti $y$-nal. Ha azonosak (illetve kongruensek modulo $n$), elfogadja Biankának az $n$ prímtényezőinek ismeretére vonatkozó állítását.

Jó-e Bianka tudásának ez a bizonyítása? Vizsgáljuk meg alaposan. Ellenőrizzük néhány feltétel teljesülését!

1. *Elemér a protokoll szabályai szerint eljárva nem tudhat meg semmit* Bianka titkáról; amit megtudhat, az az egyetlen bitnyi információ, hogy Bianka tudja-e a titkot, vagy nem. Ez rendben van, Elemér valóban nem tudott meg semmit, hisz Bianka olyan számot küldött vissza, amit Elemér már egyébként is ismert.
2. *Bianka nem csaphatja be Elemért.* Erre Biankának valóban nincs módja. Az egyetlen lehetősége, hogy $v^4$-re $v^2$-tel válaszol.

3. *Elemér nem adhatja ki magát egy harmadik személy előtt, mint Bianka titkának tudója.* Ha ki tudná adni magát, az azt jelentené, hogy meg tudja határozni egy szám négyzetgyökét, akkor pedig $n$ felbontását is meg tudja adni, azaz tud(hat)ja a titkot. Az természetesen előfordulhat, hogy Elemér egy olyan számot kap, amelynek négyzetgyökére „véletlen" próbálkozással rátalál, ennek valószínűsége azonban rendkívül kicsi. (Olyan támadás persze elképzelhető, hogy valaki Bianka felé ellenőrnek, míg vele egy időben Elemér felé bizonyítónak adja ki magát, és Elemér üzenetét változatlanul átküldi Biankának, míg az ő válaszát Elemérnek küldi. Az ilyen támadás ellen más, e protokollon kívüli módszert kell használni.)
4. *Elemér nem csaphatja be Biankát.* Ez azt jelenti, hogy Elemér a protokoll szabályaitól való eltéréssel nem juthat információhoz. Ez a feltétel sajnos esetünkben nem teljesül! Ha Elemér egy olyan $y$ számot választ (és ilyet $1/2$ valószínűséggel véletlenül is találhat, mint a 6. feladatban), mely nem négyzetelem, és $-y$ sem, akkor a válaszul kapott $w$ és ellentettje, $-w$, együtt megadják $y^2$ négy négyzetgyökét, aminek ismeretében Elemér már felbonthatja $n$-et tényezői szorzatára.
5. *A protokollt ismerő külső megfigyelő még azt sem tudhatja meg, hogy Bianka tudja-e a titkot*[5]. Ez másként fogalmazva azt jelenti, hogy a valóságos párbeszédek könnyen szimulálhatók olyannal, melyek a titok ismerete nélkül készültek és megkülönböztethetetlenek a valóságosaktól. Esetünkben e feltétel is fennáll, hisz $(v^4, v^2)$ párokat bárki generálhat a prímtényezők ismerete nélkül is, és e számokkal lejátszhatja a fenti protokollt.

E részben sikertelen, de tanulságos próbálkozás után másik módszerrel próbálkozunk.

### 3.2. Használjuk, amit a varázslóktól tanultunk

Látjuk, az előző megoldás nem volt jó abban az értelemben, hogy Elemér – igaz, csak a protokoll szabályainak be nem tartásával – megszerezhette Bianka titkát. Eszerint olyan megoldást kell találnunk, melyben Bianka nem vállalja, hogy egy Elemér által javasolt számból négyzetgyököt von. Ez hasonló ahhoz, ahogy Bebió

[5] E feltételt nevezik angolul „zero knowledge condition"-nek.

sem vállalta, hogy bármely állatot átvarázsol bármivé. Ő azt tette, hogy előbb az Ellea által adott állatot titokban átvarázsolta valami mássá. Meg tudjuk ezt mi is valósítani az Elemér által választott négyzetszámmal?

Az ötlet az, hogy a megadott négyzetszámot Bianka először beszorozza egy véletlenül választott szám négyzetével, és csak ebből vállalja a modulo $n$ vett négyzetgyökvonást. A javított protokoll tehát a következő. Adva van $x \in \mathbb{Z}_n^*$, ahol $n$ két különböző prím szorzata. Bianka bizonyítja, hogy ismer olyan $t \in \mathbb{Z}_n^*$ számot, melyre $x \equiv t^2 \pmod{n}$, azaz ismeri $x$ valamely négyzetgyökét.

*1. lépés:* Bianka választ egy véletlen $v \in \mathbb{Z}_n^*$ számot, és elküldi Elemérnek az $y = v^2 x \bmod n$ számot. (Bianka „átvarázsolja" az $x$ négyzetszámot egy másik négyzetszámmá.)

*2. lépés:* Elemér választ egy véletlen $b$ bitet (azaz $b = 0$ vagy 1), és azt elküldi Biankának. (A $b = 0$ eset felel majd meg a „viszka"-kérés esetének.)

*3. lépés:* Bianka visszaküldi a $w = vt^b \bmod n$ értéket Elemérnek. (Eszerint $b = 0$ esetén Elemér megtudja, hogy melyik $v$ szám négyzetével „varázsolta" Bianka $x$-et $y$-ná, $b = 1$ esetén pedig megtudja $y$ egy négyzetgyökét.)

*4. lépés:* Elemér ellenőrzi, hogy $b = 0$ esetén fennáll-e a $w^2 x \equiv y \pmod{n}$, míg $b = 1$ esetén a $w^2 \equiv y \pmod{n}$ kongruencia. Ha nem áll fenn, nem fogadja el Bianka állítását.

Vizsgáljuk meg ezt a protokollt is!

1. *Aki tudja $t$ értékét, $b$ bármilyen választása mellett sikeresen le tudja játszani a protokollt.* Valóban, $t$ ismeretében $y$ és $w$ kiszámítása $b$ egyik értéke mellett sem okoz nehézséget.
2. *Bárki, aki $t$ értékét nem ismeri (például az imposztor Imre), minden körben csak 1/2 valószínűséggel jár sikerrel a bizonyító szerepében.* Ha Imre megsejti, hogy $b$ értéke 0 lesz, választ egy véletlen $r$ számot, s a protokoll szabályait követve sikerrel jár. Ha Imre megsejti, hogy $b = 1$ lesz, akkor választ egy véletlen $w$ számot, és az 1. lépésben Elemérnek az $y = w^2 \bmod n$ számot küldi. A 3. lépésben a $w$ számot küldi, ami a 4. lépésben sikert hoz számára.
3. *A protokoll során semmi új információhoz sem lehet jutni.* Fidél, aki nagyon figyeli a párbeszédeket, és persze semmit nem

tud a titokból, $b = 0$ esetén lát egy $(y, w) = (v^2 x, v)$ számpárt, míg $b = 1$ esetén egy $(y, w) = (w^2, w)$ számpárt. Ezek mind olyan számpárok, amilyeneket maga is tudna generálni tetszőleges, akár előre adott bitsorozathoz, $b = 0$ esetén egy véletlenül választott $v$, míg $b = 1$ esetén egy véletlen $w$ szám segítségével.

E protokoll nemcsak akkor használható, ha Bianka bármely szám négyzetgyökét ki tudja számolni, de akkor is, ha csak egyetlen $x$ szám egyetlen $g$ négyzetgyökét tudja, amiből még nem tudja meghatározni $n$ prímfelbontását. Egy ilyen tudás bizonyításának egy lehetséges alkalmazásáról szól a következő fejezet.

### 3.3. Személyazonosítás

Ez a protokoll takarékosabban fog bánni azzal az információval, amit egy nagy szám prímtényezős alakjának ismerete jelent, itt ugyanis nem a prímtényezők ismerete lesz a titok, vagy ami ezzel ekvivalens, a gyököt vonni tudás, hanem csak egyetlen szám négyzetgyökének ismerete.

A következő protokoll egyszerre több ember számára is lehetővé teszi, hogy személyazonosságukat igazolják. Egy megbízható központ keres két nagy – legalább százjegyű – $p$ és $q$ prímet, kiszámítja az $n = pq$ számot, a $p$ és $q$ számokat megsemmisíti, majd nyilvánosságra hozza $n$-et. Minden azonosítandó $S$ személynek ad egy $t$ számot, mely 0 és $n - 1$ közé esik, és amelyre $(t, n) = 1$. Ez lesz a személy titkos kódja. Az $x = t^2 \bmod n$ számot $S$ nevével együtt nyilvánosságra hozza, ez lesz $S$ nyilvános azonosító száma.

Ha Elemér azonosítani akarja Biankát, akkor megkéri, bizonyítsa be, hogy tudja a neki adott titkos $t$ számot. E bizonyítás több körben, a következő lépések néhányszori megismétlésével történik:

*1. lépés:* Bianka választ egy véletlen $v$ egészt, és elküldi Elemérnek az $y = v^2 \bmod n$ számot.

*2. lépés:* Elemér választ egy véletlen $b$ bitet, azaz a 0 vagy az 1 számok valamelyikét, és ezt elküldi Biankának.

*3. lépés:* Bianka válaszul elküldi az $w = vt^b$ számot, vagyis ha $b = 0$, akkor a $v$, ha $b = 1$, akkor a $vt$ számot.

*4. lépés:* Elemér ellenőrzi, hogy fennáll-e a $w^2 \equiv yx^b \pmod{n}$ kongruencia. Ha nem, nem fogadja el, hogy Bianka ismeri $t$-t, azaz nem hiszi el, hogy valóban ő Bianka.

### 3.4. Pénzfeldobás telefonon keresztül

Lehet-e telefonon keresztül „fej vagy írás”-t játszani? Bianka feldob egy érmét, Elemér megtippeli telefonon keresztül, majd Bianka megmondja, hogy jó-e a tipp. Nem tűnik valami biztonságos játéknak. Arra volna szükségünk, hogy Bianka, miután feldobta a pénzt, küldje el a dobás eredményét Elemérnek, de úgy kódolva, hogy Elemér azt semmiképpen se tudja megfejteni, majd Elemér tippje után küldje el Elemérnek a dekódoláshoz szükséges kulcsot is, amivel Elemér megtudhatja, hogy mi volt Bianka dobásának eredménye. Ráadásul Elemérnek a dekódolás után látnia kell azt is, hogy Bianka nem rendelkezhet egy másik kulccsal is, aminek segítségével a másik eredmény jönne ki. Ez épp olyan, mint amikor a sakkozók borítékolják a lépést, amelyet majd csak egy későbbi időpontban lehet felnyitni, tartalmát addig nem lehet megtudni, utána viszont nem lehet letagadni. Először egy bitnyi információ *borítékolás*ára mutatunk egy protokollt, mely a négyzetes maradék problémáról írtakra épül.[6]

Bianka választ egy $n = pq$ alakú számot, ahol $p, q > 2$ prímek, és egy $m \in \mathbb{Z}_n^*$ álnégyzetelemet. $p$ és $q$ értékét titokban tartja, de $n$ és $m$ értékét nyilvánosságra hozza. Ezután Bianka a következőképpen tud egy $b$ bitet borítékolni. Először választ egy véletlen $x \in \mathbb{Z}_n^*$ egészt, és elküldi Elemérnek az $m^b x^2 \bmod n$ számot (ez lesz a borítékolt bit). Egy későbbi időpontban Bianka elküldi a $b$ és $x$ számokat Elemérnek, amivel „felnyitja” a borítékot.

Vegyük észre, hogy $m^0 x^2$ négyzetelem, $m^1 x^2$ viszont álnégyzet. Amennyiben a négyzetes maradék probléma „nehéz”, Elemér nem tudja megállapítani, hogy a Biankától kapott szám négyzet vagy álnégyzet, tehát nem tudja, hogy $b$ értéke 0 vagy 1. Másrészt Bianka nem tud csalni, ahhoz ugyanis az kéne, hogy egy borítékolt üzenetet kétféleképpen is fel tudjon nyitni, úgy is, hogy $b = 0$, úgyis, hogy $b = 1$ legyen. Ha ez lehetséges volna, akkor létezne két $x_1$ és $x_2$ szám, hogy $mx_1^2 \equiv x_2^2 \pmod{n}$, és így $m \equiv (x_2 x_1^{-1})^2 \pmod{n}$ volna, ami nem lehet, hisz $m$ nem négyzetelem.

E protokollal már nem lesz nehéz a „fej vagy írás” játékot lejátszani telefonon. Legyen például 0 a fej, 1 az írás. Legyen $p =$

[6] Hasonló kérdésről – a kártyaosztás telefonon keresztül való megvalósíthatóságáról – szól a KöMaL egy érdekes cikke [1].

= 271, $q$ = 479, így $n$ = 129809. $p$ és $q$ ismeretében könnyen ellenőrizhető, hogy például $m$ = 68017 álnégyzet. Bianka választ egy véletlen $x$ számot, legyen ez mondjuk 1000, feldob egy pénzt, fej esetén ($b$ = 0) a 91337-et, írás esetén a 69607-et mondja a telefonba Elemérnek. Elemér tippel, ezután Bianka elküldi a $b$ értékét, ami 0 vagy 1, és a véletlenül választott $x$ számot[7].

A borítékolás nemcsak a pénzfeldobásban használható protokoll. Utolsó feladatunkban arra kérjük az Olvasót, hogy maga konstruáljon egy bizonyos matematikai ismerethez nem feltáró bizonyítást.

Legyen $\mathcal{G}$ egy gráf, mely csúcspontok egy $V$ halmazából és bizonyos csúcspárokat összekötő élek egy $E$ halmazából áll. A kérdés: kiszínezhetők-e a gráf csúcsai 3 színnel úgy, hogy bármely két – $E$-beli él mentén – szomszédos csúcs különböző színű legyen.

*10. feladat.* Bianka azt állítja, hogy ismeri egy adott $\mathcal{G}$ gráf csúcsainak 3-színezését (ami azt jelenti, hogy a gráf csúcsai úgy vannak kiszínezve, hogy bármely él két végpontja különböző színű legyen). Adjunk meg egy kriptográfiai protokollt, mellyel Bianka nem feltáró bizonyítását adhatja tudásának. A protokollban az alábbi jelöléseket használjuk: a csúcsok száma $|V| = v$, az éleké $|E| = k$. $V$ elemei, azaz a csúcsok 1-től $v$-ig meg vannak sorszámozva. A három színt 2-jegyű bináris sorszámukkal jelöljük, nevezetesen az első, második, illetve harmadik színt a 01, 10, illetve 11 bináris szám jelöli. A gráf színezését egy $b_1b'_1b_2b'_2 \dots b_vb'_v$ bitsorozat formájában adják meg, ahol $b_ib'_i$ az $i$-edik csúcs színének 2-jegyű kódja.

[7] Bár e számok lényegesen kisebbek, mint amekkorákat a biztonság megkövetel, bizonyos körülmények között a fentihez hasonló nagyságú számokkal is működik a játék, például ha Bianka csak a játék kezdetén közli Elemérrel $n$ és $m$ értékét, és Elemérnél csak egy – a négy alapművelet kiszámolására képes – zsebszámológép van.

## 4. A feladatok megoldásai

*1.* Ha csak annyit kell Biankának bizonyítania, hogy ki tudja nyitni a $C$ kaput, akkor elég, ha Elemér elkíséri a $B$ elágazásig, ott megáll, míg Bianka besétál a barlangba az egyik elágazáson, majd kijön a másikon. Ha azonban nem szeretnék, hogy az Elemért kísérő Fidél is megtudja, hogy Bianka tudja-e a titkot vagy nem, akkor a következőképp járnak el: az $A$ bejáratnál Elemér (és Fidél) vár, míg Bianka bemegy a barlang $C$ kapujáig. Ekkor Elemér bemegy a $B$ pontig, és ott kihívja Biankát a barlang valamelyik ágán. Ha nem azon jön ki, Bianka nem tudja a titkot. Ha ott jön ki, megismétlik az eljárást néhányszor. Fidél számára semmi sem bizonyítja, hogy amit lát, nemcsak egy előre megbeszélt színjáték.

*2.* Az eredmény

$$242424242^{-1} \bmod 12121212121 = 1154401152.$$

Megadjuk a számításokhoz használt táblázatot:

| | | |
|---|---|---|
| 12121212121 | 0 | |
| 242424242 | 1 | $(\lfloor \frac{12121212121}{242424242} \rfloor = 50)$ |
| 21 | $-50$ | $(\lfloor \frac{242424242}{21} \rfloor = 11544011)$ |
| 11 | 577200551 | |
| 10 | $-577200601$ | |
| 1 | 1154401152 | |

*3.* Először a korábban tanult módszerrel meghatározzuk a $7^{-1} \bmod 11$ és a $11^{-1} \bmod 7$ inverzeket. Igen rövid számolás után – de akár fejben próbálgatással is – kapjuk, hogy $7^{-1} \bmod 11 = 8$ és $11^{-1} \bmod 7 = 4^{-1} \bmod 7 = 2$. Az $x = aq\bar{q}_p + bp\bar{p}_q$ képletbe helyettesítve kapjuk, hogy $x = 2 \cdot 11 \cdot 2 + 3 \cdot 7 \cdot 8 = 212$, de $212 \equiv 58 \pmod{77}$, így a kongruenciarendszer összes megoldása leírható az $x \equiv 58 \pmod{77}$ kongruenciával, illetve felírható $x = 58 + 77k$ alakban, ahol $k$ tetszőleges egész. A másik kongruenciarendszer megoldása hasonló számítás után $x = -2 \cdot 11 \cdot 2 - 3 \cdot 7 \cdot 8 = -212$, de $-212 \equiv 19 \pmod{77}$ miatt az összes megoldása

$x \equiv 19 \pmod{77}$ alakba, illetve $x = 19 + 77k$ alakba írható, ahol $k$ tetszőleges egész.

*4.* Mivel $\frac{31+1}{4} = 8$, ezért a négyzetgyökök $\pm 2^8 \bmod 31$, illetve $\pm 5^8 \bmod 31$. A 8-dik hatvány kiszámítható 3 négyzetreemeléssel. Ezek eredményi 4, 16, 8, illetve 5, 15, 5, tehát 2 négyzetgyökei 8 és 23 ($23 \equiv -8 \pmod{31}$), míg 5 négyzetgyökei 25 és 6 ($6 \equiv -25 \pmod{31}$).

*5.* Tekintsük először az $x^2 \equiv 53 \pmod{7}$ és az $x^2 \equiv 53 \pmod{11}$, illetve a velük ekvivalens $x^2 \equiv 4 \pmod{7}$ és $x^2 \equiv 9 \pmod{11}$ kongruenciákat! Ezek megoldásai $\pm 2$, illetve $\pm 3$, amit fejben számolva is azonnal látunk, de megkaphatjuk a $\pm 4^{\frac{7+1}{4}} \bmod 7$, illetve a $\pm 9^{\frac{11+1}{4}} \bmod 11$ hatványok kiszámolásával is. Ezek után tehát az alábbi négy kongruenciarendszert kell megoldanunk:

$$\text{(1)} \quad \begin{aligned} x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{11} \end{aligned} \qquad \text{(2)} \quad \begin{aligned} x &\equiv 2 \pmod{7} \\ x &\equiv -3 \pmod{11} \end{aligned}$$

$$\text{(3)} \quad \begin{aligned} x &\equiv -2 \pmod{7} \\ x &\equiv 3 \pmod{11} \end{aligned} \qquad \text{(4)} \quad \begin{aligned} x &\equiv -2 \pmod{7} \\ x &\equiv -3 \pmod{11} \end{aligned}$$

Az (1) és a (4) kongruenciarendszert már megoldottuk a *3. feladat*ban, a megoldás 58, illetve 19. A másik két rendszer hasonlóan oldható meg, a megoldások 30 és 47. Tehát 53 négyzetgyökei modulo 77 számolva: 19, 30, 47, 58.

*6.* Válasszunk egy véletlen $v \in \mathbb{Z}_n^*$ elemet, és legyen $a = v^2 \bmod n$. Az $f$ eljárás segítségével határozzuk meg egyik gyökét. Annak valószínűsége, hogy $f$ nem ad új gyököt, azaz hogy $f(a) = v$ vagy $f(a) = -v$ épp $1/2$, míg $1/2$ annak a valószínűsége is, hogy $f(a) \neq \pm v$, tehát $a$ négy gyöke: $\pm v$, $\pm f(a)$. Így a fenti eljárás $k$-szori megismétlése után $1/2^k$ annak az esélye, hogy sikertelenül járunk.

*7.* Álnégyzetelem, hisz $19 \equiv 5 \pmod{7}$, míg $19 \equiv 8 \pmod{11}$, és az Euler-feltétellel azonnal látható, de fejben is könnyen

ellenőrizhető az összes lehetőség végigszámolásával, hogy 5 nem négyzetelem modulo 7, és 8 nem négyzetelem modulo 11. $\mathbb{Z}_{77}^*$ négyzetelemeinek listája: 1, 4, 9, 15, 16, 23, 25, 36, 37, 53, 58, 60, 64, 67, 71. Az álnégyzetek listája: 6, 10, 13, 17, 19, 24, 40, 41, 52, 54, 61, 62, 68, 73, 76.

*8.* Az 58 négyzetelem, a többi nem. Ennek bizonyítását az Euler-feltétel is elvégezhetjük (ld. 11. old.), de egyszerűbb számítás is elég. Ha $x_0$ az egyik gyök, és $x_0$ négyzetelem, akkor kielégíti az $x^2 \equiv x_0 \pmod{77}$ kongruenciát, de akkor kielégíti a $x^2 \equiv x_0 \pmod 7$ és a $x^2 \equiv x_0 \pmod{11}$ kongruenciákat is. Ezek szerint az előző feladat megoldásában megadott négy kongruenciarendszer közül azt kell kiválasztani, melynek mindkét kongruenciájában négyzetelem áll a jobb oldalon. Könnyű ellenőrizni, hogy ez csak az (1) kongruenciarendszerre áll, tehát ennek megoldása, vagyis 58 az egyetlen négyzetelem modulo 77.

*9.* Ha $a \in S$, akkor $a$ négyzetelem modulo $p$ és modulo $q$ is, azaz az Euler-feltétel szerint $a^{(p-1)/2} \equiv 0$ vagy $1 \pmod p$ és $a^{(q-1)/2} \equiv 0$ vagy $1 \pmod q$. Eszerint

$$\left(a^{\frac{(p-1)(q-1)+4}{8}}\right)^2 = \left(a^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} a \equiv a \pmod p$$

és hasonlóképpen

$$\left(a^{\frac{(p-1)(q-1)+4}{8}}\right)^2 = \left(a^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}} a \equiv a \pmod q.$$

Ezekből következik, hogy

$$\left(a^{\frac{(p-1)(q-1)+4}{8}}\right)^2 \equiv a \pmod n,$$

ami bizonyítja, hogy az $x \in S \mapsto x^2 \bmod n$ leképezés $S$ egy permutációja, és hogy inverze az $x \in S \mapsto x^{\frac{(p-1)(q-1)+4}{8}} \bmod n$ leképezés.

*10.* Az alábbi lépéseket elegendően sokszor – legalább $k^2$-szer – megismétlik:

*1.* Bianka véletlen sorrendbe állítja a színeket, és e színkiosztás mellett előállítja a $b_1 b_1' b_2 b_2' \dots b_v b_v'$ bitsorozatot (ilyenből

összesen 6 létezik, veszi tehát ezek egyikét). A fenti bitsorozat minden $b$ bitjéhez választ egy véletlen $x_b \in \mathbb{Z}_n^*$ elemet, és a már ismert módon, az $m^b x_b^2 \bmod n$ képlettel borítékolja. Végül a borítékolt bitek sorozatát elküldi Elemérnek.

2. Elemér választ egy $(i, j)$ élt, ahol $i$ és $j$ egy-egy csúcs sorszáma.
3. Bianka visszaküldi a kiválasztott két csúcs borítékolt bitjei kibontásához szükséges információkat, azaz a $(b_i, x_{b_i})$, $(b'_i, x_{b'_i})$, $(b_j, x_{b_j})$, $(b'_j, x_{b'_j})$ számpárokat.
4. Elemér ellenőrzi, hogy a két csúcs helyesen van-e kódolva, és hogy valóban különböző színűek-e.

## Hivatkozások


[1] Bodó Zalán, Pataki János, *Kártya telefonon: avagy tanuljunk nyelveket!*, KöMaL 1985/4 145–146; *Még mindig kártyajáték telefonon, avagy fő a diszkréció*, KöMaL 1985/5 193–196. (`http://www.sulinet.hu/komal`)

[2] Freud Róbert, Gyarmati Edit, *Számelmélet*, Nemzeti Tankönyvkiadó, 2000.

[3] Ködmön József, *Kriptográfia*, ComputerBooks, 1999.

[4] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997. (A könyv teljes anyaga megtalálható az interneten is a `http://cacr.math.uwaterloo.ca/hac/index.html` címen.)

[5] Sárközy András, *Számelmélet és alkalmazásai*, Műszaki Könyvkiadó, 1978.

[6] S. Singh, *Kódkönyv*, Park Kiadó, 2001.

[7] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.

[8] Szalay Mihály, *Számelmélet*, TypoTEX, Nemzeti Tankönyvkiadó, 1998.