Eötvös Loránd Tudományegyetem
Természettudományi Kar

Karkus Zsuzsa
Matematika BSc
Matematikus szakirány

Fedőrendszerek

Szakdolgozat

Témavezető: Freud Róbert egyetemi docens

Budapest, 2013.

Tartalomjegyzék

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek, Freud Róbertnek javaslatait, kérdésfelvetéseit és a dolgozat alapos átnézését. Valamint Hermann Péternek, a latex használatához nyújtott segítségét.

Bevezetés

Az egész számokat szeretnénk lefedni különböző modulusú maradékosztályokkal. Vagyis maradékosztályok

$$a_i \pmod{m_i}, \quad 1 < m_1 < m_2 < ... < m_k$$

rendszerét fedőrendszernek nevezzük, ha minden egész szám eleme legalább az egyik maradékosztálynak. A fedőrendszereket Erdős definiálta, egy Romanov által feltett kérdés megválaszolásához. A kérdés a következő: létezik-e végtelen sok olyan páratlan szám, amely nem $2^k + p$ alakú, ahol p prím és k természetes szám. Erdős egy fedőrendszert használt annak az erősebb állításnak a bizonyítására, hogy létezik olyan páratlan számokból álló végtelen számtani sorozat, amelynek egyik tagja sem áll elő ilyen alakban. Számos megoldatlan probléma van fedőrendszerekkel kapcsolatban, ezek közül a két leghíresebb, Erdős pénzdíjas probléma a következő:

1. Van-e olyan fedőrendszer, amelynek minden modulusa páratlan?

2. Létezik-e minden K pozitív egészhez olyan fedőrendszer, amelynek minden modulusa legalább K?

A második kérdéssel kapcsolatban a legjobb eredmény jelenleg Nielsen konstrukciója $K = 40$-re. Ez a konstrukció több mint 10^{50} modulust használ. A dolgozat első részében leírjuk Nielsen módszerének alapötletét és ennek alapján konstruálunk egy fedőrendszert, amelynek a legkisebb modulusa 12.

A második részben a fedőrendszerek egy általánosításával, többdimenziós fedőrendszerekkel foglalkozunk.

Először mutatunk egy módszert, amellyel többdimenziós fedőrendszereket konstruálhatunk olyan egydimenziós fedőrendszerekből, melyeknek minden modulusa összetett szám. Nem csak ezzel a módszerrel lehet többdimenziós fedőrendszereket konstruálni, erre mutatunk két példát. Az első Schinzel konstrukciója egy kicsit módosítva, felhasználva Nielsen akkor még nem ismert konstrukcióját, amelyben a legkisebb modulus 40. A másodikat Simpson módszerét használva konstruáljuk.

A 2.5. fejezetben megmutatjuk, hogy vannak olyan n-dimenziós fedőrendszerek, amelyek nem triviálisan kaphatók egy 2-dimenziós fedőrendszerből.

A dolgozatban megválaszoljuk Simpson [6]-ban feltett kérdését (2.3.2. Tétel), valamint önállóan is felteszünk néhány kérdést, amelyeket meg is válaszolunk (2.1.3. Definíció előtt, 2.4.11. Megjegyzés, 2.5.7. Megjegyzés).

Végül felvetünk néhány további kérdést.

1. Fedőrendszer nagy legkisebb modulussal

1.0.1. Definíció. *Maradékosztályok*

$$a_i \pmod{m_i}, \quad 1 < m_1 < m_2 < ... < m_k$$

rendszerét fedőrendszernek nevezzük, ha minden x egész számra $x \equiv a_i \pmod{m_i}$ valamely i-re.

Fedőrendszerekkel kapcsolatban rengeteg kérdés felmerül. Például ha nem tennénk fel, hogy minden modulus különböző, foglalkozhatnánk olyan fedőrendszerekkel, amelyek minden számot pontosan egyszer fednek le (ilyen nem létezik, ha a modulusok különbözőek). Híres megoldatlan kérdés, hogy létezik-e olyan fedőrendszer, amelynek modulusai páratlan számok. Mi most a következő, Erdős által feltett, máig megoldatlan kérdéssel fogunk foglalkozni:

Létezik-e minden K pozitív egészhez olyan fedőrendszer, amelynek minden modulusa legalább K?

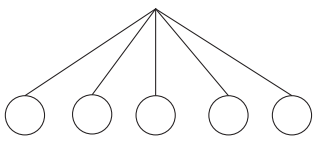
Sokan konstruáltak olyan fedőrendszert, amelynek minden modulusa legalább K egy adott K-ra. Az eddigi legjobb eredmény Nielsen konstrukciója $K = 40$-re [2]. (Korábban $K = 25$ volt a rekord).

Ebben a részben először ismertetjük Nielsen módszerét, majd ennek alapján konstruálunk egy fedőrendszert, amelynek legkisebb modulusa 12. Teszünk néhány utalást, hogy a konstrukciót hogyan lehetne változtatni, hogy 12-t növelni tudjuk. De azt is látni fogjuk, hogy a helyzet lényegesen bonyolultabbá válik, ha 12-t jelentősen növeljük. Nielsen munkája alapján úgy sejti, hogy Erdős kérdésére nemleges a válasz.

Először bevezetünk néhány jelölést, amelyek majd megkönnyítik a fedőrendszer leírását.

1.1. Jelölések

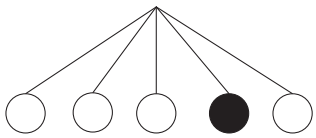
Gráfszerű ábrákkal fogjuk lerajzolni a maradékosztályokat. Például, ha szeretnénk ábrázolni a maradékosztályokat modulo 5, akkor egy 5 ágú fát rajzolunk, az ágak végén körökkel:



1. ábra.

Ugyanígy, bármely p prím esetén a maradékosztályokat modulo p egy p ágú fával fogjuk ábrázolni. Az első ág felel meg $1 \pmod p$-nek, a második $2 \pmod p$-nek, és így tovább, a p-edik $p \pmod p$-nek.

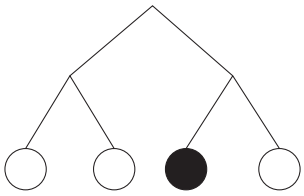
Ha azt akarjuk jelölni, hogy egy maradékosztály le van fedve modulo p, a neki megfelelő kört feketére színezzük. Például, ha $4 \pmod 5$ van fedve, az ábra:



2. ábra.

Bevezetünk egy másik jelölést is, az előző példa ezzel a jelöléssel:
$5(-,-,-,1,-)$. Az 5 a modulust jelenti, a maradékosztályoknak megfelelően 5 input van, ha az i. helyen 1-es van, az azt jelenti, hogy az $i \pmod{5 \cdot 1}$, vagyis az $i \pmod 5$ maradékosztály le van fedve.

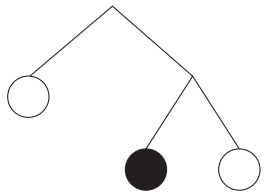
Most megnézzük, hogyan változnak a jelölések, ha egy prímhatvány modulusú maradékosztályt akarunk lefedni, például $2 \pmod 4$-et. Először rajzolunk egy kétágú fát (a modulo 2 maradékosztályoknak megfelelően), aztán mindkét ágat további két ágra bontjuk a modulo 4 maradékosztályok szerint:



3. ábra.

Így kaptunk 4 kört, ami megfelel a maradékosztályoknak modulo 4. Az első kettő azoknak felel meg, amelyek az $1 \pmod 2$ maradékosztályba tartoznak (növekvő sorrendben), vagyis az első két kör az $1 \pmod 2$-t és a $3 \pmod 2$-t jelenti. A második két kör azoknak a maradékosztályoknak felel meg, amelyek $2 \pmod 2$-be tartoznak, tehát $2 \pmod 4$-nek és $4 \pmod 4$-nek. Tehát a $2 \pmod 4$-et úgy jelöljük, hogy először lemegyünk a $2 \pmod 2$-nek megfelelő jobb oldali ágon, aztán a $2 \pmod 4$-nek megfelelő (bal oldali) ágon és azt a kört feketére színezzük. (A többi kör üresen marad.)

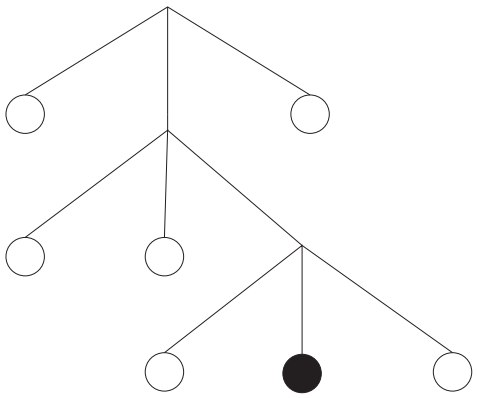
Mivel az $1 \pmod 2$ ágon nincs fekete kör, az ottani ágakat felesleges is megrajzolni, tehát így is ábrázolhatjuk:



4. ábra.

Ennek megfelelően a másik jelölésben is írhatunk $2(-,2(1,-))$-t. A külső kettes második inputjába írtunk, ez jelenti azt, hogy a 2 (mod 2) ágon vagyunk, a belső $2(1,-)$ jelöli, hogy ezen belül melyik ágon vagyunk (nevezetesen az első, vagyis a 2 (mod 4)-nek megfelelő ágon), a modulus pedig $2 \cdot 2 = 4$.

Ugyanígy a $3(-,3(-,-,3(-,1,-)),-)$ 17 (mod 27)-et jelenti. Könnyű ábrázolni:

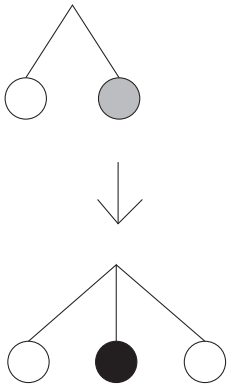


5. ábra.

Most tegyük fel, hogy a modulusunk több prímmel is osztható. A kínai maradéktételből tudjuk, hogy egy maradékosztályt modulo $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, ahol $p_1 < \dots < p_r$ különböző prímek, $\alpha_1, \dots, \alpha_r \in \mathbb{N}$, egyértelműen meghatároz alkalmas modulo $p_i^{\alpha_i}$ maradékosztályok metszete.

Ha a modulusunk $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ mint fentebb, a gráfos jelölés esetén először lerajzoljuk, hogy melyik ágon vagyunk $p_1^{\alpha_1}$ szerint, (p_1 a legkisebb prím), aztán alá külön ábrán, hogy melyik ágon vagyunk $p_2^{\alpha_2}$ szerint, és így tovább a prímek szerinti növekvő sorrendben.

Tehát például 2 (mod 6) esetén az ábra:



6. ábra.

A szürke kör azt jelenti, hogy az a maradékosztály (itt $2 \pmod 2$), csak részben van fedve.

A másik jelölésnél, ha a modulusunk $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ mint fentebb, kívül a legnagyobb prímmel, p_r-rel és hatványaival kezdünk, majd haladunk befelé a prímekkel csökkenő sorrendben. Tehát $2 \pmod 6$ esetén a jelölésünk: $3(-,2(-,1),-)$.

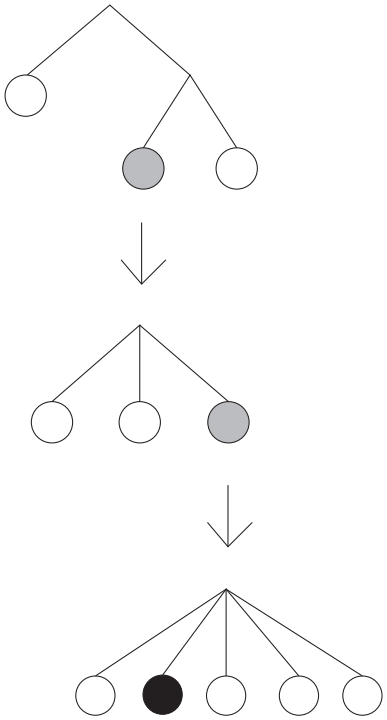
Azért választottuk ezeket a jelöléseket, mert a konstrukciónkban a prímekkel növekvő sorrendben fogunk foglalkozni, és így ha egy új prímet nézünk, az inputjaiban csak olyan prímek fognak szerepelni, amelyeket már megtárgyaltunk, így könnyebb lesz elkerülni, hogy egy modulust többször is használjunk.

Nézzünk még egy példát:
Melyik maradékosztályt jelöli $5(-,3(-,-,2(-,2(1,-))),-,-,-)$?
A modulus a prímek szorzata: $5 \cdot 3 \cdot 2 \cdot 2 = 60$. Ábrázolni könnyű, lásd a 7. ábrát.

A keresett maradékosztály $2 \pmod 4$, $3 \pmod 3$ és $2 \pmod 5$ metszete. Kis számolás után kapjuk, hogy $42 \pmod{60}$.

Gyakran egyszerűsíteni fogunk a jelöléseinken, például, ha tudjuk, hogy egy prímhatvány szerint melyik ágon vagyunk. Mondjuk, ha a $3 \pmod 4$ ágon vagyunk, és $7 \pmod{12}$-t szeretnénk jelölni, akkor nem írjuk ki a teljes $2(2(-,1),-)$-t, hanem a helyére csak a 4-et írjuk, vagyis $3(4,-,-)$ az egyszerűsített jelölés. Tehát ha egy prímhatvány szerint tudjuk, hogy melyik ágon vagyunk, a rá vonatkozó résznél nem írunk mást, csak a prímhatványt.

Egy másik egyszerűsítés, hogy ha például lefedtük $1 \pmod{10}$-et és $4 \pmod 5$-öt is, akkor nem külön-külön írjuk le, hogy $5(2(1,-),-,-,-,-)$ és $5(-,-,-,1,-)$, hanem írhatjuk egybe is: $5(2(1,-),-,-,1,-)$.



7. ábra.

1.2. Az alapötlet

Ebben a részben bemutatunk olyan módszereket, amelyeket lehet használni fedőrendszerek konstruálásakor. Először kimondunk egy önmagában is érdekes tételt:

1.2.1. Tétel. *Egy fedőrendszer modulusai legyenek* $m_1, m_2, \ldots, m_n$.
Ekkor $\sum_{i=1}^{n} \frac{1}{m_i} > 1$.

Bizonyítás. I. Először belátjuk, hogy $\sum_{i=1}^{n} \frac{1}{m_i} \geq 1$. Az $m_1, \ldots, m_n$ modulusok legkisebb közös többszörösét jelöljük l-lel. Az m_i modulusú maradékosztály az első l szám közül $\frac{l}{m_i}$-t fed le. A fedőrendszerünk az összes számot lefedi 1-től l-ig, tehát $\sum_{i=1}^{n} \frac{l}{m_i} \geq l$. Osztva l-lel: $\sum_{i=1}^{n} \frac{1}{m_i} \geq 1$.

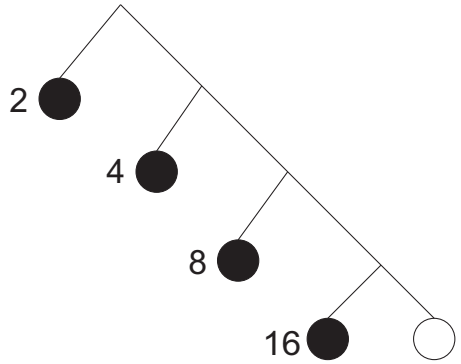
II. Még be kellene látni, hogy $\sum_{i=1}^{n} \frac{1}{m_i} \neq 1$. Ehhez elég, hogy nincs olyan fedőrendszer, amely minden számot pontosan egyszer fed. Ennek a bizonyítását nem részletezzük. (Lásd például [3]-ban.) □

1.2.2. Következmény. *Nem létezik olyan fedőrendszer, amelynek modulusai egyetlen prím különböző hatványai, mivel minden* p *prímre* $\sum_{i=1}^{\infty} \frac{1}{p^i} \leq \sum_{i=1}^{\infty} \frac{1}{2^i} = 1$.

1.2.3. Megjegyzés. *A következményhez már a gyengébb* $\sum_{i=1}^{n} \frac{1}{m_i} \geq 1$ *is elég, ugyanis a fedőrendszerünkben csak véges sok modulus lehet, tehát ezek reciprokösszege kisebb, mint* $\sum_{i=1}^{\infty} \frac{1}{p^i} \leq 1$.

A következmény ellenére most mégis kezdjünk el konstruálni egy olyan rendszert, amelynek modulusai kettőhatványok.

Először vegyünk be a rendszerbe egy 2 modulusú maradékosztályt, mondjuk 1 (mod 2)-t. Most válasszunk egy 4 modulusút, az 1 (mod 4) és a 3 (mod 4) már le van fedve, tehát válasszunk egyet a maradék kettő közül, mondjuk 2 (mod 4)-et. Modulo 8 ismét két olyan maradékosztály van, ami még nincs lefedve, válasszuk 4 (mod 8)-at. Modulo 16 válasszuk 8 (mod 16)-ot. Vagyis eddig 2(1,2(1,2(1,2(1, −)))) van fedve. Ábrázolva:



8. ábra.

Folytatjuk ezt az eljárást, megint két lehetőség közül választhatunk modulo 16, válasszuk 8 (mod 16)-ot, és így tovább, válasszuk 2^{k-1} (mod 2^k)-t, $k = 1, \ldots, n$.

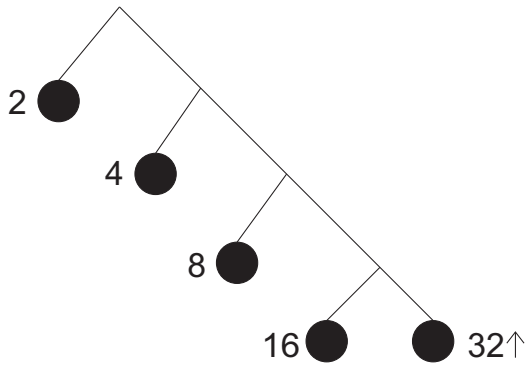
Akármilyen véges lépésben ez nem lesz fedőrendszer, de már csak 2^n (mod 2^n)-t kellene lefednünk ahhoz, hogy az legyen, valamely kellően nagy n-re. Ehhez felhasználunk egy p prímszámot (vagy egy kettőhöz relatív prím számot). Általában p-t nagyra fogjuk választani. Legyen $n \geq p - 1$. Minden $1 \leq i \leq p$-re tekintsük az i (mod p) és a 2^{n+1-i} (mod 2^{n+1-i}) maradékosztályok metszetét. A kínai maradéktétel szerint ez egy maradékosztály modulo $2^{n+1-i}p$. A jelölésünkkel kifejezve: $p(2^n,2^{n-1},\ldots,2^{n-(p-1)})$-t tekintjük, ahol a kettőhatványok inputjait nem írtuk ki, mivel itt most világos, hogy melyik ágon vagyunk modulo 2^{n+1-i}, $i = 1, \ldots, p$. Mivel $2^{n+1-i}p$, $i = 1, \ldots, p$-re különböző modulusok, és a fent leírt maradékosztályok együtt lefedik 2^n (mod 2^n)-t, tehát ezzel együtt már fedőrendszert kapunk.

Általában n-et jóval nagyobbra fogjuk választani $p-1$-nél, ekkor minden modulus $p(2^n, ...,2^{n-(p-1)})$-ben osztható lesz egy nagy kettőhatvánnyal, ami segíteni fog, hogy ne ismételjünk modulust.

Ezt a módszert később sokat fogjuk használni, ezért bevezetünk rá egy jelölést. Az így leírt rendszert 2 ↑-lal jelöljük.

Most tegyük fel, hogy le szeretnénk fedni egy maradékosztályt modulo 2^{m-1}. Erre az esetre is be fogunk vezetni egy jelölést. Egy maradékosztály modulo 2^{m-1} két maradékosztály uniója modulo 2^m. Az egyiket vegyük be a fedésbe. A másik, két maradékosztály uniója modulo 2^{m+1}, az egyiket bevesszük a fedésbe, a másikat tovább bontjuk, és így tovább, végül egy maradékosztály marad fedetlenül modulo 2^n, egy kellően nagy n-re. Ezt pedig le tudjuk fedni a fentebb leírt módszerrel egy nagy p prímszám, vagy kettőhöz relatív prím szám segítségével. Vagyis pontosan ugyanazt csináltuk, mint 2 ↑-nál, csak most egy adott ágon voltunk modulo 2^{m-1}. Ezek alapján (2^m) ↑ jelentse azt, hogy vesszük a megfelelő maradékosztályokat a következő modulusokkal: $2^m, 2^{m+1}, ..., 2^n$ és $p2^n, p2^{n-1}, ..., p2^{n-(p-1)}$, ahol p egy nagy prím (vagy egy kettőhöz relatív prím) és $n \geq p-1$. Általában n-et most is nagyra fogjuk választani, hasonló okokból, mint 2 ↑-nál.

Ezzel a jelöléssel az előző ábrán az üres kört (16 (mod 16)) tudjuk fedni 32 ↑-lal.



9. ábra.

Nézzünk egy konkrét példát. Leírjuk, hogy pontosan melyik maradékosztályok tartoznak 2 ↑-hoz, $n = 2$ és $p = 3$ esetén:

$$
\begin{array}{rlcrll}
1 & (\text{mod } 2), & & & & \\
2 & (\text{mod } 4), & & & & \\
(1 & (\text{mod } 3)) & \cap & (4 & (\text{mod } 4)) = 4 & (\text{mod } 12), \\
(2 & (\text{mod } 3)) & \cap & (2 & (\text{mod } 2)) = 2 & (\text{mod } 6), \\
(3 & (\text{mod } 3)) & \cap & (1 & (\text{mod } 1)) = 3 & (\text{mod } 3).
\end{array}
$$

Ez valóban fedőrendszer.

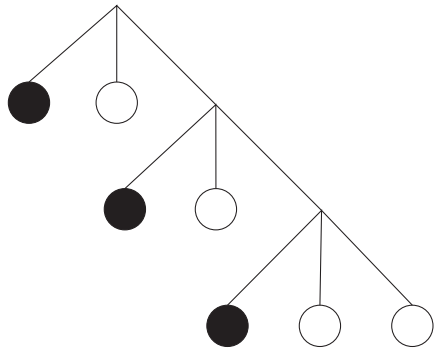
Most nézzük meg, mi történik, ha növeljük n-et. Tehát 2 ↑ $n = 3$ és $p = 3$ esetén:

$$1 \pmod 2, \quad 2 \pmod 4, \quad 4 \pmod 8,$$
$$16 \pmod{24}, \quad 8 \pmod{12}, \quad 6 \pmod 6.$$

Láthatjuk, hogy most minden modulus osztható kettővel. Ahogy n-et tovább növeljük, a nem kettőhatvány modulusok oszthatóak lesznek egyre nagyobb kettőhatványokkal, mint ahogy azt már korábban is megjegyeztük.

A nyíl jelölést be szeretnénk vezetni 2-nél nagyobb prímekre is. Itt egy kicsit más lesz a helyzet, például nézzük meg $q = 3$-ra. Mint ahogy azt a kettőnél is tettük, először elkezdünk felírni egy olyan rendszert, amelynek modulusai különböző hatványai 3-nak.

Most azonban, ha mindig csak egy maradékosztályt választunk modulo 3^k, $k = = 1, ..., n$, akkor rengeteg maradékosztály marad fedetlenül. Például, ha az $1 \pmod 3$, $3 \pmod 9$, $9 \pmod{27}$ rendszert választottuk, akkor ez ábrázolva:



10. ábra.

Ez így nem fog működni. Viszont, ha mindig két maradékosztályt fedünk le modulo 3^k, $k = 1, ..., n$, akkor csak egy maradékosztály marad fedetlenül modulo 3^n, ezt pedig le tudjuk fedni egy nagy prím, vagy egy 3-hoz relatív prím számot felhasználva, ugyanúgy, ahogy a $2 \uparrow$-nál tettük.

A jelölésnél vegyük figyelembe, hogy most mindig két maradékosztályt fedtünk le minden szinten, vagyis szükség van két inputra, ahol jelöljük, hogy mivel fedjük le ezeket. Vagyis a jelölés $3 \uparrow (-, -)$, az üres inputokat megfelelően kitöltve.

Ugyanez működik tetszőleges q prímre. Ha most $q-1$ maradékosztályt fedünk le modulo q^k, $k = 1, ..., n$-re, akkor csak egy fedetlen lyuk marad modulo q^n (nevezetesen $q^n \pmod{q^n}$), amit le tudunk fedni egy q-hoz relatív prím szám segítségével. És ahogy a 3-nál 2 inputra volt szükségünk, most $q - 1$ inputra van szükség, tehát a jelölés: $q \uparrow (-, ..., -)$.

A $q \uparrow$-at definiálhatjuk egy végtelen rekurzióval is:

$$q \uparrow (\alpha_1, \alpha_2, ..., \alpha_{q-1}) = q(\alpha_1, \alpha_2, ..., q \uparrow (\alpha_1, \alpha_2, ..., \alpha_{q-1}))$$

Ez így végtelen sok maradékosztályt ad, de a fentebb leírt módszerrel a rendszer végessé tehető egy q-hoz relatív prím nagy p segítségével.

1.2.4. Megjegyzés. *Ezt a definíciót a gráfos ábrázolással a legkönnyebb elképzelni: ha ábrázolni akarjuk a q $\uparrow$-at, a rekurzív definíció alapján rajzolunk q darab ágat, az első $q-1$-nél $q\uparrow$ inputjai alapján tudjuk, melyik maradékosztályokról van szó, a q. ágnál meg megint a $q\uparrow$ szerepel, a rekurzív definíció alapján megint rajzolunk q darab ágat, az első $q-1$-nél megint tudjuk, melyik maradékosztályokról volt szó, és így tovább. Véges sok lépés után megállunk, ekkor csak egy ág van az ábra alján, amelyről nem tudjuk, melyik maradékosztályok fedik le, de $q\uparrow$ definíciójába beleértjük, hogy ezt az utolsó ágat mivel fedjük le, nevezetesen egy nagy prímszám (vagy egy q-hoz relatív prím) segítségével, ugyanúgy, ahogy azt $2\uparrow$-nál is tettük.*

Most mutatunk egy példát, leírjuk a maradékosztályokat $3\uparrow(1{,}2\uparrow)$-ban.
Ehhez először nézzük meg $2\uparrow$-at $n=5$ és $p=5$-tel. Ebben az esetben a fedésünk:

$$\begin{aligned} T=\{&1 \pmod 2, \quad 2 \pmod 4, \quad 4 \pmod 8, \quad 8 \pmod{16},\\ &16 \pmod{32}, \quad 96 \pmod{160}, \quad 32 \pmod{80}, \quad 8 \pmod{40},\\ &4 \pmod{20}, \quad 10 \pmod{10}\}. \end{aligned}$$

Ezután, ha $(a \pmod m)\cap T$-t írunk (m relatív prím a T-ben szereplő modulusok mindegyikéhez), az alatt azokat a maradékosztályokat értjük, amelyeket úgy kapunk, hogy $a \pmod m$-et metsszük egy T-beli maradékosztállyal.

Legyen S azoknak a maradékosztályoknak a halmaza, amelyeket $3\uparrow(1{,}2\uparrow)$ határoz meg. A rekurziós definíció szerint

$$3\uparrow(1{,}2\uparrow)=3(1{,}2\uparrow,3\uparrow(1{,}2\uparrow)),$$

amiből azt kapjuk, hogy $1 \pmod 3$ benne van S-ben, és a második input $2\uparrow$, tehát $(2 \pmod 3)\cap T$ benne van S-ben. Ismét alkalmazzuk a rekurziót:

$$3(1{,}2\uparrow,3\uparrow(1{,}2\uparrow))=3(1{,}2\uparrow,3(1{,}2\uparrow,3\uparrow(1{,}2\uparrow))),$$

amiből láthatjuk, hogy $3 \pmod 9$ és $(6 \pmod 9)\cap T$ benne van S-ben.

A rekurziót folytatva látszik, hogy $3^{k-1} \pmod{3^k}$ és $(2\cdot 3^{k-1} \pmod{3^k})\cap T$ benne van S-ben $k=1{,}2,\ldots$-ra. Megállhatunk $k=4$-nél, mivel az ekkor egyetlen fedetlen lyukat, $3^4 \pmod{3^4}$-t be tudjuk fedni az 5-öt használva a $3\uparrow(-,-)$ definíciójánál leírt módon, vagyis $5(3^4{,}3^3{,}3^2{,}3{,}1)$-gyel. (Ebben használtuk az $5\cdot 3=15$ modulust).

T-ben 10 modulust használtunk fel, S-ben pedig 49-et. Ha $3\uparrow$-ban vagy $2\uparrow$-ban p-t nem 5-re, hanem nagyobbra választottuk volna, vagy n-et választottuk volna nagyobbra, még több modulust használtunk volna fel.

Nézzük meg, mi történne, ha T konstruálásánál $n = 5$ helyett $n = 4$-et választottunk volna. Vagyis legyen T' az a fedés, amelyet 2 $\uparrow$-ból kapunk $n = 4$ és $p = 5$ esetén.

$$\begin{aligned} T' = \{&1 \pmod 2, \quad 2 \pmod 4, \quad 4 \pmod 8, \quad 8 \pmod{16}, \\ &56 \pmod{80}, \quad 12 \pmod{40}, \quad 18 \pmod{20}, \quad 9 \pmod{10}, \\ &5 \pmod 5\}. \end{aligned}$$

T' használja az 5-öt modulusként, tehát ha $3 \uparrow (1{,}2 \uparrow)$-hoz T helyett T'-t használtuk volna, akkor a 15-öt kétszer is felhasználtuk volna modulusként, vagyis így nem kaptunk volna fedőrendszert.

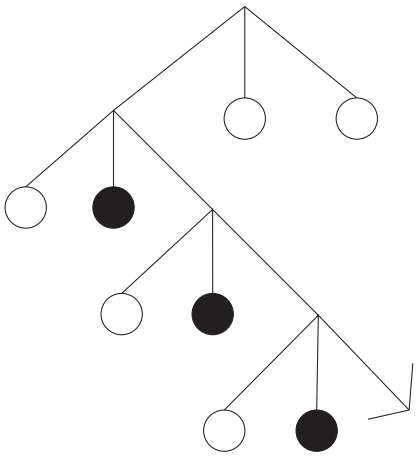
Azzal, hogy n-et növeljük, már megoldódik a probléma ebben az esetben, de ez nem minden esetben lesz elég. Sokféleképpen elkerülhetjük, hogy egy modulust többször is használjunk a q $\uparrow$-akhoz választandó p prímek (vagy q-hoz relatív prímek) miatt, például minden nyílhoz használhatunk különböző prímeket. De megtehetjük azt is, hogy minden q $\uparrow$-hoz ugyanannak a nagy prímnek különböző hatványait használjuk, mivel bármilyen q-hoz relatív prím megfelel. Amikor lehetséges, mint például a $3 \uparrow (1{,}2 \uparrow)$ példánál, használhatjuk ugyanazt a prímet is. Mivel a konstrukcióban sokszor fogunk valamilyen q $\uparrow$-at használni, így rengeteg modulust kell felhasználnunk.

Szeretnénk bevezetni a (2^m) $\uparrow$-hoz hasonló jelölést, kettőnél nagyobb q prímekre. (2^m) $\uparrow$-at úgy defniáltuk, hogy egy meghatározott ágon voltunk modulo 2^m, és ezt befedtük $2 \uparrow$ módszerével. Ugyanezt fogjuk csinálni $q > 2$ esetén is. Tegyük fel, hogy egy meghatározott ágon vagyunk modulo q^{m-1}. Most ugyanazt csináljuk mint q $\uparrow$-nál, vagyis $q-1$ maradékosztályt lefedünk modulo q^k, $k = m, ..., n$ egy elég nagy n-re. A fedetlenül maradt maradékosztályt modulo q^n pedig lefedjük egy nagy, q-hoz relatív p prím segítségével. Most is szükségünk van $q - 1$ inputra, tehát a jelölés: $q^m \uparrow (-, ..., -)$.

Pontosabban megfogalmazva, ha az $a \pmod{q^{m-1}}$ ágon vagyunk, akkor q^m $\uparrow$-nak a j-edik inputja alatt $(1 \leq j \leq q - 1)$ a következő maradékosztályokat értjük:

$$a + jq^{k-1} - q^{m-1} \pmod{q^k}, \quad k \geq m. \tag{1.2.1}$$

Mutatunk egy példát. Tegyük fel, hogy az $1 \pmod 3$ ágon vagyunk modulo 3. Ekkor $9 \uparrow (-{,}1)$ a régi jelölésünkkel egyenlő a következővel: $3(3 \uparrow (-{,}1), -, -)$. Ábrázolva:



11. ábra.

Az első fekete kör az $1 + 2 \cdot 3 - 3 \pmod 9$ maradékosztály. Azt, hogy a k-adik szinten lévő fekete kör az $1 + 2 \cdot 3^{k-1} - 3 \pmod{3^k}$ maradékosztálynak felel meg, láthatjuk indukcióval. $k = 2$-re igaz. Tegyük fel, hogy igaz k-ra. A $k+1$-edik szinten lévő fekete kört úgy kapjuk, hogy $1 + 2 \cdot 3^{k-1} - 3$-hoz hozzáadunk 3^{k-1}-t (így a k. szinten lévő jobb szélső kört kapjuk), és még hozzáadunk 3^k-t. Így a $k + 1$-edik szinten lévő fekete kört kapjuk, ami ezek szerint a következő maradékosztálynak felel meg: $1 + 2 \cdot 3^{k-1} - 3 + 3^{k-1} + 3^k = 1 + 2 \cdot 3^k - 3 \pmod 3$. Vagyis tényleg (1.2.1)-et kaptuk $a = 1$, $j = 2$ és $q = 3$-mal.

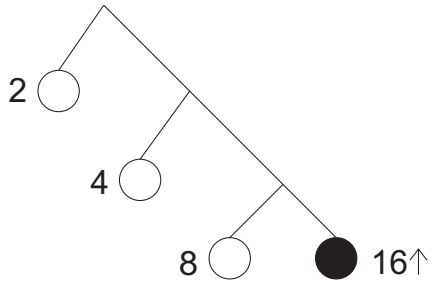
1.3. A konstrukció

Nielsen konstrukciója 40-es legkisebb modulusra meglehetősen bonyolult, ezért a módszerét egy egyszerűbb eseten mutatjuk be. Konstruálunk egy olyan fedőrendszert, amelynek legkisebb modulusa 12. Hogy könnyebben számon tudjuk tartani, mely modulusokat használtuk már, sorba vesszük a prímeket, és mindegyiknél leírjuk, hogy mit fedünk le vele.

2

A kettőt arra használjuk, hogy a $2 \uparrow$ által meghatározott kongruenciákkal lefedjük az egész számokat. Mivel olyan fedőrendszert szeretnénk, amelynek legkisebb modulusa 12, nem használhatjuk a 12-nél kisebb modulusú kongruenciákat, vagyis $1 \pmod 2$-t, $2 \pmod 4$-et és $4 \pmod 8$-at. Ezeket majd más prímek segítségével fogjuk lefedni. $16 \uparrow$-ban csak 12-nél nagyobb modulusok vannak, ezt benne hagyjuk a fedésben, így lefedtük $8 \pmod 8$-at.

Ábrázolva:

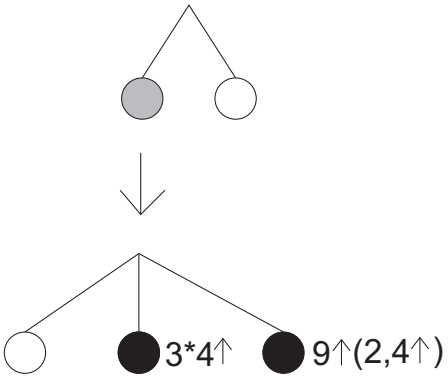


12. ábra.

3

A hármat fogjuk felhasználni, hogy részben fedjük a kettő eltávolításával keletkezett lyukat, vagyis 1 (mod 2)-t.

$3 \uparrow (2,4 \uparrow)$ lefedi 1 (mod 2)-t, csak el kell távolítanunk a 12-nél kisebb modulusokat. $3 \uparrow (2,4 \uparrow)$ azt jelenti, hogy egy meghatározott ágon vagyunk modulo 2, nevezetesen most az 1 (mod 2) ágon, és hasonlóan csináljuk, mint $3 \uparrow (1,2 \uparrow)$-nál, vagyis lefedünk két maradékosztályt most modulo $2 \cdot 3^k, \quad k = 1, ..., n$, a fedetlenül maradt maradékosztályt modulo $2 \cdot 3^n$ pedig lefedjük egy nagy prím segítségével. Azaz a következő maradékosztályok benne lesznek a fedésben: $(3^{k-1} \pmod{3^k}) \cap (1 \pmod 2)$ és $2 \cdot 3^{k-1} \pmod{3^k}$ metszve a $4 \uparrow$-beli maradékosztályokkal (ahol $4 \uparrow$ az 1 (mod 2)-t fedi). A felhasznált modulusok közül egyedül a 6 kisebb, mint 12, tehát az 1 (mod 6)-ot kivesszük a rendszerből, a többi viszont maradhat, így 2 (mod 3) $\cap$ $\cap$ $4 \uparrow$ lefedi 5 (mod 6)-ot, $9 \uparrow (2,4 \uparrow)$ pedig fedi 3 (mod 6)-ot. Tehát ábrázolva a helyzetet:



13. ábra.

A bal oldali üres kör a 6-os modulus eltávolításával keletkezett, a szürke kör pedig azt jelenti, hogy az adott maradékosztály csak részben van fedve. A fekete körök mellé van írva, hogy mivel fedtük le őket.

Ahhoz, hogy teljesen lefedjük az 1 (mod 2) maradékosztályt, csak 1 (mod 6)-ot kell fednünk. Ehhez majd a 11 és a 13 prímeket fogjuk felhasználni.

5

Az ötöt fogjuk felhasználni, hogy lefedjük a lyukat, amely a 4-es modulus eltávolításával keletkezett, nevezetesen 2 (mod 4)-et.

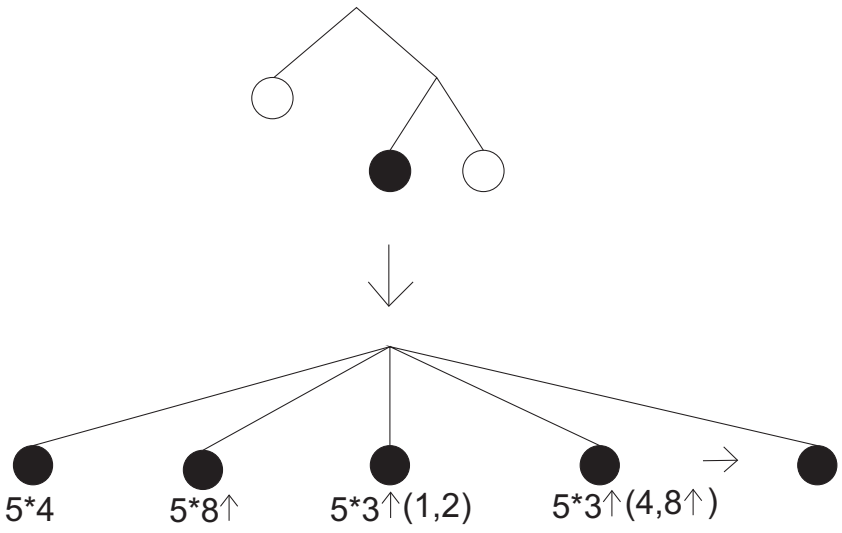
1.3.1. Megjegyzés. *Ha olyan fedőrendszert szeretnénk konstruálni, amelynek legkisebb modulusa nagyobb, mint 12, akkor az 5-öt érdemesebb a 8-as modulus elhagyásával keletkezett lyuk fedéséhez használni (ahogy Nielsen is tette a 40-es legkisebb modulus konstrukciójánál), mivel ha nem használhatnánk a kisebb modulusokat, és a* 2 (mod 4)*-et akarnánk fedni az 5-tel, túl sok új lyuk keletkezne.*

Viszont most olyan rendszert szeretnénk konstruálni, ahol a legkisebb modulus 12, és így az 5-öt felhasználva le tudjuk fedni az egész 2 (mod 4) *maradékosztályt, míg nagyobb prímet használva keletkeznének új lyukak. Tehát az 5-öt használva egyszerűbb fedőrendszert kapunk.*

Mivel most a 2 (mod 4) ágon vagyunk, 5 $\uparrow$-nak meg tudunk adni négy olyan inputot, hogy minden modulust csak egyszer használjunk, és valóban fedjük a teljes 2 (mod 4)-et:

$$5 \uparrow (4{,}8 \uparrow, 3 \uparrow (1{,}2), 3 \uparrow (4{,}8 \uparrow))$$

Ez megfelel, és mivel a 2 (mod 4) ágon vagyunk, egyértelmű, hogy a 2, a 4 és a $8 \uparrow$ melyik maradékosztályokat jelöli. Ábrázolva:



14. ábra.

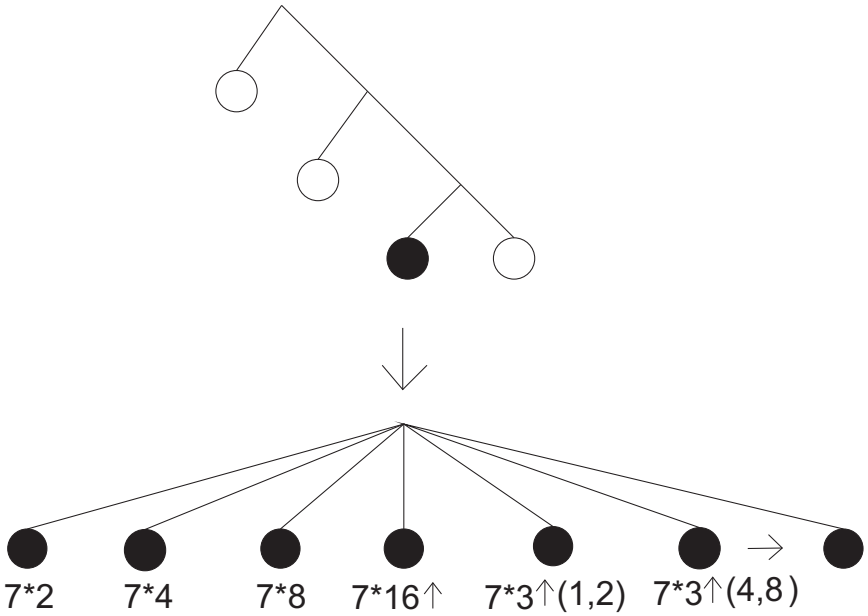
A fekete körök alá van írva, hogy mivel fedtük le őket. Az utolsó kör felé mutató nyíl azt jelenti, hogy azt $5 \uparrow$ szerint fedtük le.

7

A hetet használjuk, hogy lefedjük azt a lyukat, ami a 8-as modulus elhagyásával keletkezett. Tehát most a 4 (mod 8) ágon vagyunk, így egyértelműek lesznek a 2,4,8,16 $\uparrow$ jelölések.

$$7 \uparrow (2,4,8,16 \uparrow ,3 \uparrow (1,2),3 \uparrow (4,8))$$

lefedi 4 (mod 8)-at.
Ábrázolva:



15. ábra.

1.3.2. Megjegyzés. $7 \uparrow$ *első inputjának használhatjuk a 2-t, mivel* $7 \cdot 2 = 14 > 12$, *viszont* $5 \uparrow$ *inputjainak nem használhattuk, mivel* $5 \cdot 2 = 10 < 12$. *Mindkét esetben használhattuk az 1-et* $3 \uparrow (1,2)$*-höz, mivel* $5 \cdot 3 = 15 > 12$ *és* $7 \cdot 3 = 21 > 12$.

Tehát látható, hogy ha olyan fedőrendszert szeretnénk konstruálni, amelynek legkisebb modulusa egy kicsit is nagyobb, mint 15, akkor a helyzet bonyolódna, mivel keletkezne egy új lyuk modulo 15, melynek lefedéséhez újabb 13-nál nagyobb prímeket kellene használni, és persze az a kör, amit úgy kapunk, hogy lemegyünk az 1 (mod 2) *ágon a 13. ábrán, és aztán a középső ágon modulo 3, csak részben lenne fedve, hiszen ezt* (2 (mod 3)) $\cap$ $4 \uparrow$*-lal fedtük le, ami használja modulusként a 12-t és* $12 < 15$.

Azt könnyű megoldani, hogy a $7 \uparrow$ *inputjai között ne használjuk a 2-t, vagyis, hogy ne használjuk modulusként a 14-et, hiszen 2 helyett használhatjuk* $7 \uparrow$ *inputjaként a következőt:*

$$5 \uparrow (4,8 \uparrow ,3 \uparrow (1,2),3 \uparrow (4,8 \uparrow)).$$

Vagyis azt, amit 2 (mod 4) *fedésére is használtunk, csak most értelemszerűen a 4 és a* $8 \uparrow$ *a* 4 (mod 4) *ágra vonatkoznának.*

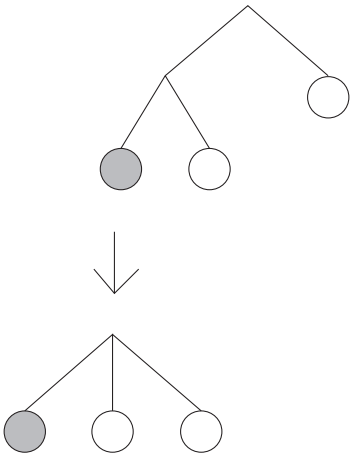
Így eddig csak egy 15-nél kisebb modulust használtunk volna, a 12-t.

Azt is érdemes megfigyelni, hogy $7\uparrow$*-ban a 2, vagy a helyette használható* $5\uparrow(4{,}8\uparrow{,}3\uparrow(1{,}2){,}3\uparrow(4{,}8\uparrow))$*, a 4, a* $3\uparrow(1{,}2)$ *és a* $3\uparrow(4{,}8)$ *helyett használható* $3\uparrow(4{,}8\uparrow)$ *az egész* $4 \pmod 4$ *maradékosztályra érvényes, amit esetleg felhasználhatnánk, ha egy nagyobb legkisebb modulusú rendszert szeretnénk konstruálni.*

11

A 11-et és a 13-at fogjuk felhasználni, hogy fedjük a lyukat, ami a 6-os modulus eltávolításával keletkezett. Most az $1 \pmod 6$ ágon vagyunk, ez két részre osztható modulo 12 szerint. A két ággal modulo 12 külön-külön fogunk foglalkozni. A 11-et fogjuk felhasználni, hogy lefedjük az $1 \pmod{12}$ ágat, és a 13-at, hogy fedjük a $7 \pmod{12}$ ágat.

A 16. ábrán jelöljük, hogy melyik ágon leszünk, amikor a 11-et használjuk.



16. ábra.

Tehát egyértelmű lesz, hogy a $2{,}4{,}8\uparrow{,}3, 6{,}12$ mire vonatkozik.

Mint ahogy azt az 5-nél és a 7-nél is tettük, a 11-nél is $11\uparrow$ inputjait fogjuk betölteni. Az első 6-ot betölthetjük a következőkkel:

$$2, \quad 4, \quad 8\uparrow, \quad 3, \quad 6, \quad 12.$$

A hetediket $9\uparrow(1{,}2)$-vel. $9\uparrow$ egy adott ágat fed (részben) modulo 3, itt fedje $1 \pmod 3$-mat. Az inputjaiban használhatjuk az 1-et, mert $11 \cdot 9^k$ alakú modulusunk még nem volt, és az ilyenek nagyobbak, mint 12, és 2-t is használhatjuk, mivel adott ágon vagyunk modulo 2, és még nem használtunk $11 \cdot 9 \cdot 2$-vel osztható modulust korábban.

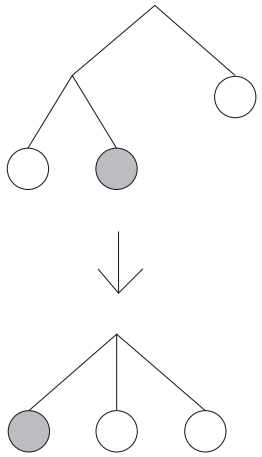
A nyolcadik inputhoz használhatjuk $9\uparrow(4{,}8\uparrow)$-at, és nem ismételtünk modulust, mivel korábban nem használtunk $11 \cdot 9 \cdot 4$-gyel osztható modulusokat, sem pedig

$11 \cdot 9 \cdot 8$-cal osztható modulusokat. A kilencedik inputhoz használhatjuk $5 \uparrow (1,2,3,4)$-et, a tizedikhez pedig $7 \uparrow (1,2,3,4,6,12)$-t.

Ezzel lefedtük $1 \pmod{12}$-t.

13

A 13-at használjuk, hogy lefedjük a 6-os modulus elhagyásával keletkezett lyuk másik részét, vagyis most a $7 \pmod{12}$ ágon leszünk. Ábrázolva:



17. ábra.

Most is $13 \uparrow$ inputjait fogjuk betölteni.

Az első 10 inputhoz a (12-ből), használjuk ugyanazokat, mint amiket $11 \uparrow$ inputjaihoz használtunk, csak most 4, $8 \uparrow$ és 12 ne ugyanazokat a maradékosztályokat jelölje, mint 11-nél, hanem a megfelelőeket, tekintve, hogy most a $7 \pmod{12}$ ágon vagyunk. A tizenegyedik inputhoz használjuk $5 \uparrow (6,8 \uparrow ,9 \uparrow (1,2),12)$-t. Nem ismételtünk modulust, mivel 13 inputjain belül 5-tel osztható modulusok csak az $5 \uparrow (1,2,3,4)$-beli modulusok voltak.

A tizenkettedik inputhoz használjuk $11 \uparrow$-at, ugyanazokkal az inputokkal, mint amikor $1 \pmod{12}$-t fedtük le, csak most a 4, $8 \uparrow$ és a 12 jelentse a megfelelő ágakat, tekintve, hogy most a $7 \pmod{12}$ ágon vagyunk. Nem ismételtünk modulust, mivel most $11 \uparrow$-at $13 \uparrow$ inputjaként használtuk, vagyis itt minden modulus osztható 13-mal.

Ezzel lefedtük $7 \pmod{12}$-t, azaz teljesen lefedtük $1 \pmod{6}$-ot. Kész a fedőrendszerünk 12-es legkisebb modulussal.

1.3.3. Megjegyzés. *Mint ahogy azt a 7-es prím tárgyalásánál is megjegyeztük (1.3.2.Megjegyzés), ha* $7 \uparrow$*-nál 2 helyett az* $5 \uparrow (4,8 \uparrow ,3 \uparrow (1,2),3 \uparrow (4,8 \uparrow))$*-at használjuk, akkor addig a 12-t kivéve nem használtunk 15-nél kisebb modulust, és*

mivel azóta sem használtunk ilyet, ha egy olyan fedőrendszert szeretnénk konstruálni, amelynek legkisebb modulusa 15, egyedül a 12-es modulus elhagyásával keletkező lyukat kéne fedni, nevezetesen $(1 \pmod 4) \cap (2 \pmod 3) = 5 \pmod{12}$*-t.*

2. Többdimenziós fedőrendszerek

2.1. Fedőrendszerek két dimenzióban

Azon (x, y) egész számpárok halmazát, amelyekre teljesül, hogy $ax+by \equiv c \pmod{m}$, jelöljük $(a, b : c : m)$-mel.

Az $S = \{(a_i, b_i : c_i : m_i), \quad i = 1,2, ..., k\}$ számnégyesek halmazát 2-dimenziós fedőrendszernek nevezzük, ha bármely $(x, y) \in \mathbb{Z}^2$-re teljesül a következő kongruenciák valamelyike:

$$\begin{aligned} a_1x + b_1y &\equiv c_1 \pmod{m_1} \\ a_2x + b_2y &\equiv c_2 \pmod{m_2} \\ &\cdot \\ &\cdot \\ &\cdot \\ a_kx + b_ky &\equiv c_k \pmod{m_k} \end{aligned}$$

továbbá $1 < m_1 < m_2 < ... < m_k$ és $\text{lnko}(a_i, b_i, c_i, m_i) = 1$. Az $m_1, m_2, ..., m_k$ számokat nevezzük a rendszer modulusainak. Az utolsó feltételre azért van szükség, mert például a következő rendszer, ha leosztunk a többi prímmel, felírható úgy is, hogy az összes modulus a 2, ezt pedig nem szeretnénk megengedni:

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ 3y &\equiv 0 \pmod{6} \\ 5x + 5y &\equiv 0 \pmod{10} \end{aligned}$$

Ha $(a_i, b_i) = (1,0)$ minden i-re, akkor egydimenziós fedőrendszert kapunk, tehát ez valóban az egydimenziós eset általánosítása.

2.1.1. Definíció. *Ha $c_i = 0, \quad i = 1,2, ..., k$-ra, akkor a rendszert homogén fedőrendszernek nevezzük. Ekkor a jelölésből is elhagyjuk c_i-t, az új jelölés: (a_i, b_i, m_i).*

Egy dimenzióban nem létezik homogén fedőrendszer, mivel végtelen sok prím van, ezért van olyan szám, amely nem osztható a véges sok modulus egyikével sem, így egyik kongruenciát sem teljesíti. Viszont két dimenzióban Cochrane és Myerson konstruált homogén fedőrendszereket egy dimenziós összetett fedőrendszerekből [4] (egy fedőrendszert összetett fedőrendszernek nevezünk, ha minden modulusa összetett szám).

Jelöljük (c, m)-mel azon x egész számok halmazát, amelyekre $x \equiv c \pmod{m}$.

2.1.2. Tétel. *Ha $\{(c_i, m_i), \quad i = 1,2, ..., k\}$ 1-dimenziós összetett fedőrendszer, $p_1, p_2, ..., p_t$ azok a prímek, amelyek osztják $\prod_{i=1}^{k} m_i$-t, akkor*

$$\{(1, -c_i, m_i), \quad (0,1, p_j), \quad i = 1, ..., k, \quad j = 1, ..., t\}$$

homogén kétdimenziós fedőrendszer.

Bizonyítás. Jelöljük M-mel a modulusok legkisebb közös többszörösét. Ha $\text{lnko}(y, M) > 1$, akkor $y \equiv 0 \pmod{p_i}$ valamely i-re. Ha $\text{lnko}(y, M) = 1$, akkor $\exists y'$, hogy $y'y \equiv 1 \pmod{M}$. Mivel $\{(c_i, m_i), \quad i = 1,2,...,k\}$ egydimenziós fedőrendszer, ezért $xy' \equiv c_i \pmod{m_i}$ valamely i-re, tehát $x - c_i y \equiv 0 \pmod{m_i}$. □

A tétel alapján elég, ha mutatunk egy egydimenziós összetett fedőrendszert, ebből már tudunk konstruálni egy kétdimenziós homogén fedőrendszert.

Selfridge konstrukciója 20 modulussal: {(0,4), (2,8), (6,16), (1,6), (5,12), (14,24), (46,48), (0,9), (15,18), (21,36), (30,72), (78,144), (3,10), (15,20), (11,15), (17,30), (59,60), (39,45), (21,90), (147,180)}.

Most megadunk végtelen sok különböző összetett fedőrendszert: Tekintsük a 2(3 ↑ (2,4 ↑),4 ↑) által meghatározott fedőrendszert. 4 ↑-nál legyen $p = 5$ és $n = 5$. Vagyis 4 ↑= {2 (mod 4), 4 (mod 8), 16 (mod 32) } ∪ 5(32,16,8,4,2). 3 ↑-on belül 4 ↑-nál szintén legyen $p = 5$ és $n = 5$, itt persze 4 ↑ 1 mod 2-re vonatkozik. 3 ↑-nál a p prím legyen legalább 7, és legyen $n = p$. Így összetett fedőrendszert kapunk. A p választására végtelen sok lehetőségünk van, és különböző p-kre különböző fedőrendszereket kapunk, mivel ha elhagynánk a p-vel osztható modulusokat, egy maradékosztály fedetlenül maradna modulo 3^n. Tehát megadtunk végtelen sok különböző összetett fedőrendszert.

2.1.3. Definíció. *Egy fedőrendszert irredundánsnak nevezünk, ha bármely kongruenciát elhagyva a rendszerből megszűnik fedőrendszernek lenni.*

Bizonyítás nélkül közöljük a következő tételt (ld. [7]):

2.1.4. Tétel. *Egy összetett fedőrendszer akkor és csak akkor irredundáns, ha a belőle konstruált homogén fedőrendszer irredundáns.*

A megadott összetett fedőrendszerek mindegyikéből konstruálhatunk egy kétdimenziós homogén fedőrendszert, és a tételből következik, hogy ezek szintén különbözőek lesznek, így megadtunk végtelen sok homogén 2-dimenziós fedőrendszert.

2.2. Fedőrendszerek n dimenzióban

2.2.1. Definíció. *Az* $S = \{(a_{i1}, a_{i2}, ..., a_{in} : c_i : m_i), \quad i = 1,2,...,k\}$ *szám n-esek halmazát n-dimenziós fedőrendszernek nevezzük, ha bármely* $x \in \mathbb{Z}^n$*-re teljesül a következő kongruenciák valamelyike:*

$$a_{i1}x_1 + a_{i2}x_2 + ... + a_{in}x_n \equiv c_i \pmod{m_i}, \quad i = 1, ..., k,$$

továbbá $m_1 < m_2 < ... < m_k$ *és* $lnko(a_{i1}, a_{i2}, ...a_{in}, c_i, m_i) = 1$. *Az* $m_1, m_2, ...m_k$ *számokat nevezzük a rendszer modulusainak.*

A homogén, irredundáns, összetett n-dimenziós fedőrendszereket ugyanúgy definiáljuk mint 2 dimenzióban.

Boping Jin és Gerry Myerson általánosította Cochrane és Myerson konstrukcióját (ld. [7]):

2.2.2. Tétel. *Legyen* $S = \{(a_{i1}, a_{i2}, ..., a_{in} : c_i : m_i), \quad i = 1,2, ..., k\}$ *egy* n*-dimenziós összetett fedőrendszer. Ekkor*

$$\{\{(a_{i1}, a_{i2}, ..., a_{in}, -c_i, m_i) : \quad i = 1,2, ..., k\}, \quad \{(0,0, ...,0,1, p_j), \quad j = 1, ..., t\}\},$$

ahol $p_1, p_2, ..., p_t$ *a prímek, amelyek osztják az* S*-beli modulusok szorzatát, egy* $n+1$*-dimenziós homogén fedőrendszer.*

A bizonyítás hasonló, mint a kétdimenziós esetben.

Felmerül a kérdés, hogy van-e olyan 2-dimenziós fedőrendszer, amely nem egy 1-dimenziós összetett fedőrendszerből származik, valamint, hogy van-e olyan n-dimenziós fedőrendszer $n > 2$-re, amely nem egy 2-dimenziós fedőrendszerből származik (például úgy, hogy $a_{ij} = 0 \quad \forall i, \quad j = 3, ..., n$). Hogy egy kicsit pontosítsunk ezeken a kérdéseken, bevezetünk egy ekvivalenciarelációt az n-dimenziós fedőrendszerek között.

2.2.3. Definíció. *Legyenek* $S = \{(a_{i1}, a_{i2}, ..., a_{in} : c_i : m_i), \quad i = 1,2, ..., k\}$ *és* $T = \{(b_{i1}, b_{i2}, ..., b_{in} : d_i : m_i), \quad i = 1,2, ..., k\}$ n*-dimenziós fedőrendszerek. Azt mondjuk, hogy* S *és* T *ekvivalens, ha létezik olyan* $F = (f_{ij}) \in \mathbb{Z}^{n \times n}$ *invertálható mátrix és* $f \in \mathbb{Z}^n$ *vektor, hogy ha az* S*-beli kongruenciákba* $x_i = \sum_{j=1}^{n} f_{ij} y_j + f_i$*-t helyettesítünk, akkor a* T*-beli kongruenciákat kapjuk:* $b_{i1}y_1 + b_{i2}y_2 + ... + b_{in}y_n \equiv d_i \pmod{m_i}, \quad i = 1,2, ..., k$ *(ha* $x = (x_1, ..., x_n)^T, \quad y = (y_1, ..., y_n)^T$ *akkor* $x = Fy +$ $+ f$*-et helyettesítünk). Ha* S *és* T *homogén, akkor* $f = 0$.

Ez tényleg ekvivalenciareláció: Reflexív: $F = Id$, $f = 0$. Szimmetrikus: ha az S-beli kongruenciákba $x = Fy + f$-et helyettesítve a T-beli kongruenciákat kapjuk, akkor a T-beli kongruenciákba $y = F^{-1}x - F^{-1}f$-et helyettesítve az S-beli kongruenciákat kapjuk. Tranzitív: ha S és T, valamint T és Z ekvivalens, és a megfelelő mátrixok és vektorok F és f, valamint G és g, akkor S és Z ekvivalenciájához jó lesz FG és $(Fg + f)$.

2.2.4. Definíció. *Legyen* S *mint fentebb és* $T = \{(b_{i1}, b_{i2}, ..., b_{ip} : d_i : m_i), \quad i = 1,2, ..., k\}$ p*-dimenziós fedőrendszer. Azt mondjuk, hogy* T *képe* S*, ha létezik* $F = (f_{ij}) \in \mathbb{Z}^{p \times n}$ *mátrix és* $f \in \mathbb{Z}^p$ *vektor, hogy ha a* T*-beli kongruenciákba* $y_i = \sum_{j=1}^{n} f_{ij} x_j + f_i, \quad i = 1, ..., p$*-t helyettesítünk, az* S*-beli kongruenciákat kapjuk.*

S-et teljesen n-dimenziós fedőrendszernek nevezzük, ha nem képe p-dimenziós fedőrendszernek semmilyen $p < n$-re.

Most már precízen meg tudjuk fogalmazni a fenti kérdéseket:

1. Van-e olyan 2-dimenziós fedőrendszer, amely nem ekvivalens olyan fedőrendszerrel, amelyet a Cochrane-Myerson-féle konstrukcióval kaptunk egy 1-dimenziós összetett fedőrendszerből?

2. Van-e teljesen n-dimenziós fedőrendszer $n > 2$-re?

2.2.5. Definíció. *Egy fedőrendszert elemi fedőrendszernek nevezünk, ha minden prím, amely osztja a modulusok szorzatát, szintén modulus.*

2.2.6. Tétel. *[7]. Legyen S $n+1$-dimenziós homogén elemi fedőrendszer:*

$$S = \{\{(a_{i1}, a_{i2}, ..., a_{in+1}, m_i),\ i = 1,2, ..., k\},\ \{(e_{j1}, e_{j2}, ..., e_{j,n+1}, p_j),\ j = 1, .., t\}\},$$

ahol m_i összetett szám minden i-re, és $p_1, ...p_t$ azok a prímek, amelyek osztják $\prod_{i=1}^{k} m_i$-t. Ekkor S ekvivalens egy olyan $n+1$-dimenziós homogén fedőrendszerrel, amelyet a Cochrane-Myerson-féle konstrukcióval kaptunk egy n-dimenziós összetett fedőrendszerből.

Bizonyítás. Legyen $g_i, \quad i = 1, ..., n+1$ a következő szimultán kongruenciarendszer megoldása:

$$\begin{aligned} x &\equiv e_{1i} \pmod{p_1} \\ x &\equiv e_{2i} \pmod{p_2} \\ &\cdot \\ &\cdot \\ &\cdot \\ x &\equiv e_{ti} \pmod{p_t} \end{aligned}$$

Legyen $G \in \mathbb{Z}^{(n+1)\times(n+1)}$ olyan invertálható mátrix, amelynek az utolsó sora $(g_1, g_2, ..., g_{n+1})$. Ekkor ha az S-beli kongruenciákba $x = G^{-1}y$-t helyettesítünk, a következő kongruenciákat kapjuk:

$$\begin{aligned} b_{i1}y_1 + b_{i2}y_2 + ... + b_{in+1}y_{n+1} &\equiv 0 \pmod{m_i}, \quad i = 1,2, ..., k, \\ y_{n+1} &\equiv 0 \pmod{p_j}, \quad j = 1, ..., t. \end{aligned}$$

Az ezek által meghatározott rendszert nevezzük T-nek. S és T ekvivalens.
$\{(b_{i1}, b_{i2}, ... : -b_{in+1} : m_i), \quad i = 1, ..., k\}$ n-dimenziós összetett fedőrendszer: legyen $z = (z_1, z_2, ..., z_n, 1) \in \mathbb{Z}^{n+1}$. Mivel z nem teljesíti egyik prím modulusú kongruenciát sem, teljesítenie kell valamelyik összetett modulusút. Tehát $b_{i1}z_1 + b_{i2}z_2 + ... + b_{in}z_n \equiv -b_{n+1} \pmod{m_i}$. T pedig ebből az n-dimenziós fedőrendszerből kapható a Cochrane-Myerson-féle konstrukcióval. □

2.3. Kétdimenziós homogén fedőrendszer kevés modulussal

Az első példánk 2-dimenziós homogén fedőrendszerre 23 modulust tartalmazott. Simpson [6]-ban megkérdezte, hogy legalább hány modulusa van egy 2-dimenziós homogén fedőrendszernek. Most ezt fogjuk megválaszolni. Először kimondunk egy Jenkin és Simpson által bizonyított tételt [8], amit fel fogunk használni.

2.3.1. Tétel. *Egy 1-dimenziós összetett fedőrendszernek legalább 20 modulusa van, és ha pontosan 20 van, akkor a modulusok legkisebb közös többszöröse 720, 1440, 2160, 2880 vagy 4320.*

Jenkin és Simpson konkrétan meg is adja, hogy egy 20 modulusú összetett fedőrendszernek mik lehetnek a modulusai, ezt most nem részletezzük, nem lesz rá szükségünk.

2.3.2. Tétel. *Egy 2-dimenziós homogén fedőrendszernek legalább 23 modulusa van.*

Bizonyítás. Indirekt tegyük fel, hogy van egy 2-dimenziós homogén fedőrendszerünk, amelynek legfeljebb 22 modulusa van. Feltehetjük, hogy ez elemi fedőrendszer, vagyis minden prím, amely osztja a modulusok szorzatát, maga is modulus. Ugyanis tegyük fel, hogy

$$ax + by \equiv 0 \pmod{pm}, \quad p \text{ prím}$$

része a rendszernek, és p nem modulus a rendszerben. Ekkor ha a fenti kongruenciát lecseréljük a következőre:

$$ax + by \equiv 0 \pmod{p},$$

akkor még mindig fedőrendszerünk van, és a modulusainak száma nem változott. (Legfeljebb csökkent, ha elhagyjuk az esetleg feleslegessé vált kongruenciákat.) Így véges sok lépésben elemi fedőrendszert kapunk, és a modulusok száma nem nőtt. Tehát ha lenne olyan nem elemi fedőrendszerünk, amelynek legfeljebb 22 modulusa van, akkor lenne ilyen elemi fedőrendszerünk is.

Most tegyük fel, hogy

$$S = \{(a_i, b_i, m_i), \quad i = 1, ..., k, \quad \{(c_j, d_j, p_j), \quad j = 1, ..., t\}\}$$

2-dimenziós homogén fedőrendszer, ahol $p_j, \quad j = 1, ..., t$ a prímek, amelyek osztják $\prod_{i=1}^{k} m_i$-t, és $k+t \leq 22$. Ekkor a 2.2.6. tétel szerint S ekvivalens egy olyan 2-dimenziós homogén fedőrendszerrel, amelyet a Cochrane-Myerson-féle konstrukcióval kaptunk egy 1-dimenziós összetett fedőrendszerből. Ennek a fedőrendszernek k modulusa van. Az első részben láttuk, hogy nincs olyan 1-dimenziós fedőrendszer, amelynek modulusai egyetlen prím különböző hatványai. A 2.2.6. Tételből következik, hogy a 2-dimenziós homogén fedőrendszerek közt sincs ilyen, ugyanis ha lenne, akkor 1-dimenziós is lenne. Tehát $t \geq 2$. Ha $t = 2$, akkor $k \leq 20$. A 2.3.1. Tételből következik,

hogy ekkor $k = 20$, és a modulusok között van 2-vel, 3-mal, illetve 5-tel osztható. De ez ellentmond annak, hogy $t \leq 2$. Most tegyük fel, hogy $t > 2$. Ekkor $k \leq 19$, de ez ellentmond a 2.3.1. Tételnek. Vagyis egy homogén fedőrendszernek legalább 23 modulusa van, és van olyan, amelynek pontosan 23 van. □

2.4. Nem elemi fedőrendszerek

2.4.1. Tétel. *Létezik olyan 2-dimenziós fedőrendszer, amely nem ekvivalens olyan fedőrendszerrel, amelyet a Cochrane-Myerson-féle konstrukcióval kaptunk egy 1-dimenziós összetett fedőrendszerből.*

Ezzel megválaszoljuk a 25. oldalon feltett 1. kérdést. A 2.2.6 tételből következik, hogy ez csak nem elemi fedőrendszer lehet, viszont egy nem elemi fedőrendszer nem lehet ekvivalens egy elemivel, mivel az ekvivalencia megőrzi a modulusokat. Tehát elég egy nem elemi fedőrendszert megadnunk. Két különböző konstrukciót fogunk mutatni olyan 2-dimenziós fedőrendszerre, amely modulusainak szorzatát osztja egy adott prím, de ez a prím maga nem modulus.

1. Schinzel konstrukciója:

Schinzel konstrukciójában (ld. [5]) az 5 osztja a modulusok szorzatát, de maga nem modulus. Ugyanezzel a módszerrel konstruálunk egy olyan rendszert, amely modulusainak szorzatát osztja a 3, de maga a 3 nem modulus. A konstrukció két 1-dimenziós fedőrendszert használ. Az egyik: $S = \{(c_i, m_i) : \quad i = 1, ..., r\}$, ahol $m_i \geq 40 \quad \forall i$. Ilyen létezik, ezt láttuk az első részben. Legyen $M = \text{lkkt}\{m_i, \quad i = = 1, ..., r\}$. A másik egy Selfridge által konstruált összetett fedőrendszer: $T = = \{(d_j, n_j), \quad j = 1, ...,21\}$, ahol $\max_j\{n_j\} = 96$ és $\text{lkkt}\{n_j \quad j = 1, ...21\} = = 1440$. Konkrétan $T = \{$(3,4), (5,8), (9,24), (9,16), (1,48), (17,32), (65,96), (3,9), (2,6), (6,18), (10,12), (18,36), (0,72), (0,10), (16,20), (12,40), (52,60), (13,15), (9,45), (4,30), (18,90)$\}$.

Állítás: a következő rendszer 2-dimenziós homogén nem elemi fedőrendszer:

$$y \equiv 0 \pmod{p}, \quad p \text{ prím}, p|10M, \quad p \neq 3, \tag{2.4.1}$$

$$y \equiv 0 \pmod{9}, \tag{2.4.2}$$

$$x - d_j y \equiv 0 \pmod{n_j}, \quad 1 \leq j \leq 21, \tag{2.4.3}$$

$$3x - c_i y \equiv 0 \pmod{3m_i}, \quad 1 \leq i \leq r, \quad 3 \not| c_i, \tag{2.4.4}$$

$$3x - (c_i + m_i)y \equiv 0 \pmod{3m_i}, \quad 1 \leq i \leq r, \quad 3|c_i, 3 \not| m_i. \tag{2.4.5}$$

Bizonyítás. A modulusok különbözőek, mivel $3m_i > n_j \quad \forall i, j$, 3 osztja a modulusok szorzatát, de maga nem modulus. Kell még, hogy minden $(x, y) \in \mathbb{Z}^2$ teljesíti valamelyik kongruenciát. Mivel a rendszer homogén, elég olyan (x, y) párokat nézni, amelyekre $\text{lnko}(x, y) = 1$. Tegyük fel, hogy $\text{lnko}(y,30) = 1$. Ekkor létezik y', hogy

$y'y \equiv 1 \pmod{30}$. Mivel T 1-dimenziós fedőrendszer, létezik j, amelyre $xy' \equiv d_j \pmod{n_j}$, tehát $x \equiv d_j y \pmod{n_j}$, vagyis (x, y) teljesíti (2.4.1)-et.
Ha lnko(y,30) > 1, akkor vagy $3|y$ vagy lnko(y,10) > 1. Az utóbbi esetben (x, y) teljesíti (2.4.1)-et $p = 2$ vagy $p = 5$-tel. Ha $3|y$, legyen $y = 3z$. Ha $3|z$, akkor (x, y) teljesíti (2.4.2)-t. Most tegyük fel, hogy $3 \not| z$. Ha lnko$(z, M) > 1$, akkor (x, y) teljesíti (2.4.1)-et. Ha lnko$(z, M) = 1$, akkor létezik z', hogy $z'z \equiv 1 \pmod{M}$. Mivel S 1-dimenziós fedőrendszer, $xz' \equiv c_i \pmod{m_i}$ valamely i-re. Vagyis $x - c_i z \equiv$ $\equiv 0 \pmod{m_i}$. Ha $3|c_i$ és $3|m_i$, akkor $3|x$, de ez lehetetlen, mivel feltettük, hogy lnko$(x, y) = 1$. Tehát $3 \not| c_i$, vagy $3 \not| (c_i + m_i)$, az első esetben (x, y) teljesíti (2.4.4)-et, a második esetben (2.4.5)-öt. (Erre az esetszétválasztásra azért volt szükség, mert az együtthatók legnagyobb közös osztójának egynek kell lennie). □

2.4.2. Megjegyzés. *Ezzel a módszerrel csak akkor tudunk olyan fedőrendszert konstruálni, amely modulusainak szorzatát osztja p, de maga a p nem modulus, ha $p = 3$ vagy $p = 5$. Ugyanis, ha $p = 2$, $\quad 2m_i > n_j$ nem teljesül például $m_i = 40$ és $n_j = 96$ esetén, ha pedig $p \geq 7$, akkor a 2.4.1-nek és a 2.4.3-nak megfelelő egyenletek:*

$$\begin{aligned} y &\equiv 0 \pmod{q}, \quad q \text{ prím, } q|30M, \quad q \neq p, \\ x - d_j y &\equiv 0 \pmod{n_j}, \quad 1 \leq j \leq 21, \end{aligned}$$

ezek közül minden $(x, y) \in \mathbb{Z}^2$ kielégít legalább egyet, tehát a többi kongruenciára nincs is szükség, így p nem osztja a modulusok szorzatát.

2. Simpson konstrukciója alapján

Először felírjuk néhány egyszerű 1 dimenzióban ismert állítás általánosítását 2 dimenzióra:

2.4.3. Lemma. *Legyenek n és m pozitív egészek, a és b egészek, úgy, hogy lnko$(a, b, nm) = 1$. Ekkor $(a, b, nm) \subseteq (a, b, m)$.*

2.4.4. Lemma. *Ha lnko$(m_1, m_2) = 1$, akkor $(a_1, b_1, m_1) \cap (a_2, b_2, m_2) = (\alpha, \beta, m_1 m_2)$, ahol $\alpha \equiv a_1 \pmod{m_1}$, $\quad \alpha \equiv a_2 \pmod{m_2}$ és $\beta \equiv b_1 \pmod{m_1}$, $\quad \beta \equiv b_2 \pmod{m_2}$.*

A konstrukció hasonló lesz, mint amit egy dimenzióban csináltunk az első részben. Egy dimenzióban egy maradékosztályt modulo p^α fel tudtunk bontani p darab maradékosztály uniójára modulo $p^{\alpha+1}$. Két dimenzióban is valami hasonlót szeretnénk.

2.4.5. Tétel. *I. A következő homogén kongruenciák uniója lefedi $(1, b, p^\alpha)$-t:*
$S = \{(0,1, p^{\alpha+1}), (1, b, p^{\alpha+1}), \{(1, b + jp^k, p^{\alpha+1}), \quad j = 1, ..., p-1, \quad k = 0, ..., \alpha\}\}$.
II. Legkevesebb $(\alpha + 1)(p - 1) + 2$ darab homogén kongruenciára van szükség ahhoz, hogy $(1, b, p^\alpha)$-t lefedjük $p^{\alpha+1}$ modulusú kongruenciákkal. (S-ben pontosan ennyi van.)

2.4.6. Következmény. $\mathbb{Z}^2 = (0,1,p) \cup (1,0,p) \cup (1,1,p) \cup \ldots \cup (1,p-1,p)$, *és legalább ennyi, azaz* $p+1$ *darab* p *modulusú kongruenciára van szükség, hogy lefedjük* $\mathbb{Z}^2$*-et.*

2.4.7. Következmény. *Ha* $p \nmid m$, *akkor egy* m *modulusú kongruencia* $p+1$ *darab* mp *modulusú homogén kongruencia uniója.*

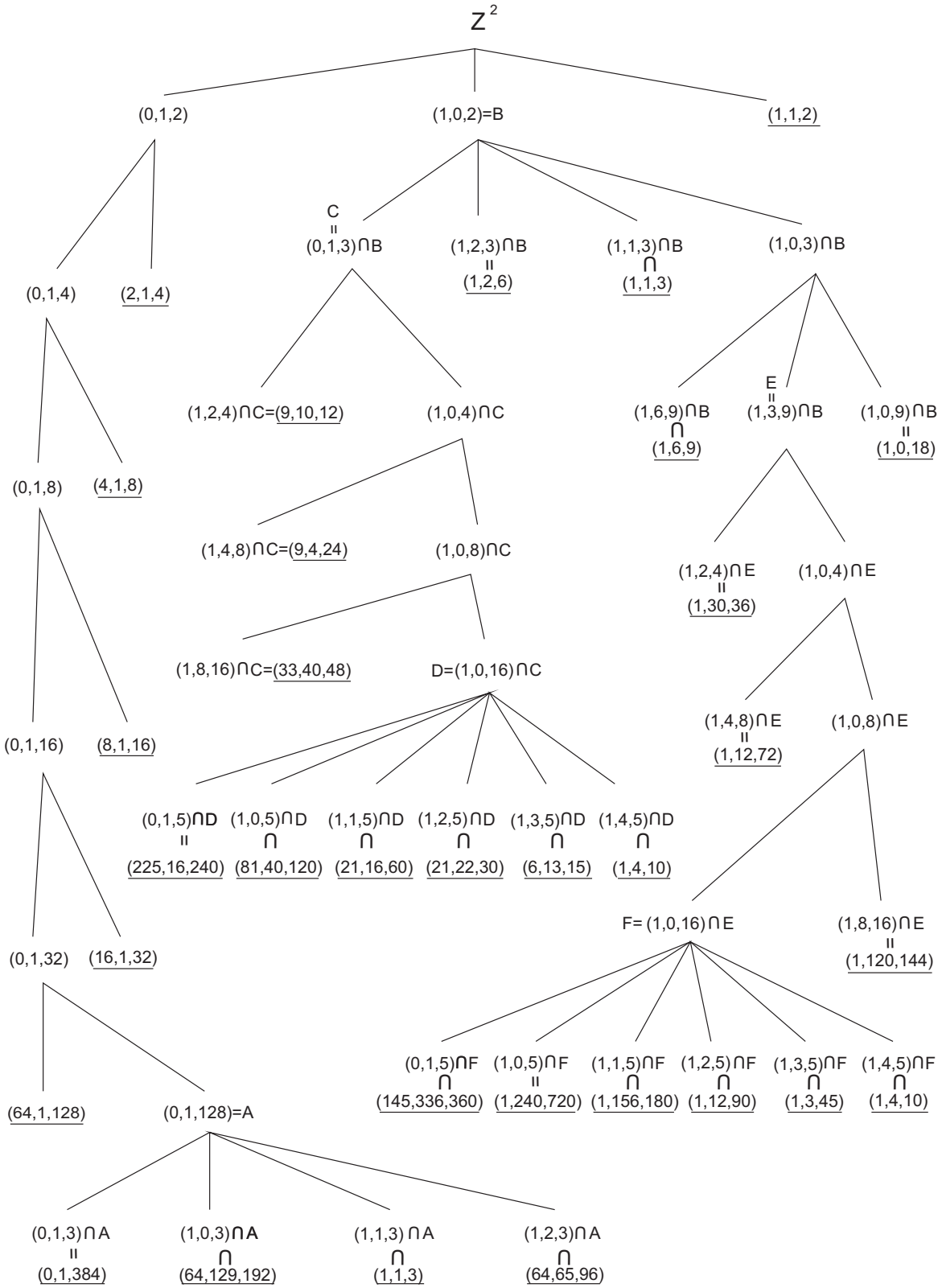
2.4.8. Tétel. *A következő homogén kongruenciák uniója lefedi* $(1, b, p^\alpha)$*-t:* $\{(1, b + jp^\alpha, p^{\alpha+1}), \quad j = 0, \ldots, p-1\}$, *és egy tetszőleges* p *modulusú homogén kongruencia.*

Bizonyítás. $(x, y) \in (1, b, p^\alpha)$, tehát $x + by \equiv 0 \pmod{p^\alpha}$. Ha $(x, y) \notin (1, b + jp^\alpha, p^{\alpha+1})$ semmilyen j-re, akkor minden j-re $x + (b + jp^\alpha)y \not\equiv 0 \pmod{p^{\alpha+1}}$, $x + (b + jp^\alpha)y = (x + by) + jyp^\alpha$, tehát ez csak úgy lehet, ha $p|y$, de ekkor $p|x$ és $\gamma x + \eta y \equiv 0 \pmod{p}$ bármilyen γ, η egészre. □

2.4.9. Megjegyzés. *Hasonló tételek igazak, ha* $(b,1,p^\alpha)$ *alakú kongruenciákat akarunk lefedni* $p^{\alpha+1}$ *modulusú kongruenciákkal.*

2.4.10. Következmény. *Ha* $p|m$, *akkor egy* m *modulusú kongruenciát lefed* p *darab* mp *modulusú és egy tetszőleges* p *modulusú kongruencia.*

Simpson bizonyította ezeket az állításokat [6], és ezeket használta a konstrukcióhoz. Mi ugyanezzel a módszerrel mutatunk egy másik példát. A konstrukciót úgy kezdjük, hogy $\mathbb{Z}^2$-et felbontjuk 2 modulusú kongruenciák uniójára: $\mathbb{Z}^2 = (0,1,2) \cup (1,0,2) \cup (1,1,2)$ (a 2.4.6. Következmény alapján). Az (1,1,2)-t bevesszük a rendszerbe, a többit tovább bontjuk. Mivel a 2 modulus a rendszerben, a 2.4.8. Tétel alapján (0,1,2) lefedhető két 4 modulusú kongruenciával. Az egyiket bevesszük a rendszerbe, a másikat tovább bontjuk két 8 modulusú kongruenciára, és így tovább, végül az egyik $2^7 = 128$ modulusú kongruenciát bevesszük a rendszerbe, a másikat a 2.4.7. Következmény alapján felbontjuk 4 darab $2^7 \cdot 3$ modulusú kongruenciára. Az egyiket bevesszük a rendszerbe, a többit az 2.4.3. Lemma alapján helyettesítjük $2^6 \cdot 3$, $2^5 \cdot 3$ és 3 modulusú kongruenciákkal. Így lefedtük (1,1,2)-t 2^k, $2^l \cdot 3$ és 3 alakú, különböző modulusú kongruenciákkal, ahol $k > 2$ és $l > 4$. Ez lényegében ugyanaz a módszer, mint az első részben a $2 \uparrow$. Most már csak (1,0,2)-t kell lefednünk. Felbontjuk 4 darab 6 modulusú kongruenciára. Ezek közül az egyik része a már a rendszerben lévő 3 modulusú kongruenciának, egy másikat beveszünk a rendszerbe, marad kettő: $(1,0,3) \cap (1,0,2)$ és $(0,1,3) \cap (1,0,2)$. Az utóbbit felbontjuk két 12 modulusúra (megtehetjük, mert a 2 modulus a rendszerben), az egyiket bevesszük a rendszerbe, a másikat tovább bontjuk két 24 modulusúra, az egyiket bevesszük, a másikat felbontjuk két 48 modulusúra, az egyiket bevesszük, a másikat felbontjuk 6 darab $5 \cdot 48 = 240$ modulusúra. Ezek közül az egyiket bevesszük a rendszerbe, a többit helyettesítjük 120, 60, 30, 15 és 10 modulusú kongruenciákkal. Most $2^k \cdot 3$ és $2^l \cdot 3 \cdot 5$ alakú modulusokat használtunk, ahol $k < 4$ és $l < 5$. Már csak $(1,0,3) \cap (1,0,2)$-t kell lefednünk. Először három 18 modulusú kongruenciára bontjuk (megtehetjük,


Z 2
(0,1,2)
(1,0,2)=B
(1,1,2)
(0,1,4)
(2,1,4)
C
=
(0,1,3)∩B
(1,2,3)∩B
=
(1,2,6)
(1,1,3)∩B
∩
(1,1,3)
(1,0,3)∩B
(0,1,8)
(4,1,8)
(1,2,4)∩C=(9,10,12)
(1,0,4)∩C
E
=
(1,6,9)∩B
∩
(1,6,9)
(1,3,9)∩B
(1,0,9)∩B
=
(1,0,18)
(1,4,8)∩C=(9,4,24)
(1,0,8)∩C
(1,2,4)∩E
=
(1,30,36)
(1,0,4)∩E
(1,8,16)∩C=(33,40,48)
D=(1,0,16)∩C
(0,1,16)
(8,1,16)
(1,4,8)∩E
=
(1,12,72)
(1,0,8)∩E
(0,1,5)∩D
=
(225,16,240)
(1,0,5)∩D
∩
(81,40,120)
(1,1,5)∩D
∩
(21,16,60)
(1,2,5)∩D
∩
(21,22,30)
(1,3,5)∩D
∩
(6,13,15)
(1,4,5)∩D
∩
(1,4,10)
F= (1,0,16)∩E
(1,8,16)∩E
=
(1,120,144)
(0,1,32)
(16,1,32)
(0,1,5)∩F
∩
(145,336,360)
(1,0,5)∩F
=
(1,240,720)
(1,1,5)∩F
∩
(1,156,180)
(1,2,5)∩F
∩
(1,12,90)
(1,3,5)∩F
∩
(1,3,45)
(1,4,5)∩F
∩
(1,4,10)
(64,1,128)
(0,1,128)=A
(0,1,3)∩A
=
(0,1,384)
(1,0,3)∩A
∩
(64,129,192)
(1,1,3)∩A
∩
(1,1,3)
(1,2,3)∩A
∩
(64,65,96)

18. ábra.

mert a 3 modulus a rendszerben), az egyiket bevesszük a rendszerbe, egy másikat helyettesítünk egy 9 modulusú kongruenciával, csak egy marad. Ezt két 36 modulusú kongruenciára bonjuk, az egyiket bevesszük a rendszerbe, a másikat megint két részre bontjuk, és így tovább, végül az egyik 144 modulusú kongruenciát bevesszük a rendszerbe, a másikat hat darab $5 \cdot 144$ modulusú kongruenciára bontjuk. Az egyiket bevesszük a rendszerbe, egy másik része egy a már a rendszerben lévő 10 modulusú kongruenciának, a többit helyettesítjük 360, 180, 90 és 45 modulusú kongruenciákkal. Ezzel készen vagyunk, lefedtük $\mathbb{Z}^2$-et különböző modulusú kongruenciákkal úgy, hogy az 5 osztja a modulusok szorzatát, de maga nem modulus. A konkrét rendszert ábrázoljuk (18. ábra). Aláhúzással jelöljük, hogy melyik kongruenciák tartoznak a rendszerbe.

2.4.11. Megjegyzés. *Amikor (0,1,2)-t fedtük le, az 5 helyett használhattunk volna bármilyen 5-nél nagyobb prímet is, csak akkor esetleg több kettőhatvány modulust kellett volna felhasználnunk. Ekkor az 5 még mindig osztja a modulusok szorzatát, de maga nem modulus, tehát nem elemi 2-dimenziós homogén fedőrendszerből is végtelen sok van.*

2.5. Teljesen n-dimenziós fedőrendszerek

Szeretnénk bebizonyítani, hogy létezik teljesen n-dimenziós fedőrendszer $n > 2$-re.

Schinzel bizonyította $n = 3$-ra, azzal a még nem bizonyított feltétellel, hogy minden k pozitív egészhez létezik olyan 1-dimenziós fedőrendszer, amelynek minden modulusa legalább k. (Ld. [5].)

Jin és Myerson bizonyította minden $n \geq 2$-re feltétel nélkül [7]. A konstrukcióhoz szükség van néhány lemmára:

2.5.1. Lemma. *Minden $d \geq 2$-re minden $(x_1, ..., x_d) \in \mathbb{Z}^d$ teljesít legalalább egyet a következő kongruenciák közül:*

$$x_i \equiv 0 \pmod 3, \qquad i = 1, ..., d, \tag{2.5.1}$$

$$x_i + x_{i+1} \equiv 0 \pmod 3, \qquad i = 1, ..., d-1, \tag{2.5.2}$$

$$x_1 \equiv x_d \pmod 3. \tag{2.5.3}$$

Bizonyítás. $x \in \mathbb{Z}^d$ teljesíti (2.5.1)-et, ha valamelyik koordinátája osztható 3-mal. Ha ez nem teljesül, és van két szomszédos koordinátája, amelyek különböző maradékot adnak modulo 3, akkor (2.5.2)-t teljesíti valamely i-re, különben minden koordináta ugyanazt a maradékot adja modulo 3, speciálisan x teljesíti (2.5.3)-at is. □

2.5.2. Lemma. *Ha lnko(m,3) = 1, akkor minden $(x_1, ...x_n, y_1, ..., y_d) \in \mathbb{Z}^{n+d}$, amely teljesíti az $a_1x_1 + ... + a_nx_n \equiv c \pmod{2^{2d-1}m}$ kongruenciát, teljesíti a következő kongruenciák valamelyikét is:*

$$(a_1x_1 + ... + a_nx_n \equiv c \pmod{2^{2d-i}m}) \wedge \qquad (y_i \equiv 0 \pmod 3, \qquad i = 1, ..., d) \tag{2.5.4}$$

$$(a_1x_1 + ... + a_nx_n \equiv c \pmod{2^{d-i}m}) \wedge (y_i + y_{i+1} \equiv 0 \pmod 3, \quad i = 1, ..., d-1) \tag{2.5.5}$$

$$(a_1x_1 + ... + a_nx_n \equiv c \pmod m) \qquad \wedge \qquad (y_1 \equiv y_d \pmod 3). \tag{2.5.6}$$

Bizonyítás. Ezt a rendszert úgy kapjuk, hogy a 2.5.2. Lemma-beli kongruenciákat metsszük olyan kongruenciákkal, amelyeknek része $a_1x_1+...+a_nx_n \equiv c \pmod{2^{2d-1}m}$, mivel csak a modulusukat cseréltük $2^{2d-1}m$ osztóira. (A $\wedge$ jellel azt fejezzük ki, hogy a bal és jobb oldalán lévő kongruenciákat egyszerre teljesítő $\mathbb{Z}^{n+d}$-beli vektorokról van szó. Ezért van szükség a lnko(m,3) = 1 feltételre is.) □

2.5.3. Megjegyzés. *A lemma igaz marad, ha néhány y-t azonosítunk egy-egy x-szel.*

Példa: A 2.5.2.Lemmában legyen $n = 2$ és $d = 3$, $(x_1, x_2) = (x, y)$, $(y_1, y_2, y_3) = = (x, y, z)$ és $m = 10$. Tegyük fel, hogy $(x, y, z) \in \mathbb{Z}^3$-re $x + y \equiv 0 \pmod{320}$. Ekkor (x, y, z) teljesíti az alábbi hat kongruencia valamelyikét:

$$\begin{array}{rcrl|rcrl}
x+y & \equiv & 0 & \pmod{320} & \wedge & x & \equiv & 0 \pmod 3, \\
x+y & \equiv & 0 & \pmod{160} & \wedge & y & \equiv & 0 \pmod 3, \\
x+y & \equiv & 0 & \pmod{80} & \wedge & z & \equiv & 0 \pmod 3, \\
x+y & \equiv & 0 & \pmod{40} & \wedge & x+y & \equiv & 0 \pmod 3, \\
x+y & \equiv & 0 & \pmod{20} & \wedge & y+z & \equiv & 0 \pmod 3, \\
x+y & \equiv & 0 & \pmod{10} & \wedge & x & \equiv & z \pmod 3.
\end{array}$$

Ezek megegyeznek a következő kongruenciákkal:

$$\begin{array}{rcll}
x + 321y & \equiv & 0 & \pmod{960}, \\
321x + y & \equiv & 0 & \pmod{480}, \\
81x + 81y + 159z & \equiv & 0 & \pmod{240}, \\
x + y & \equiv & 0 & \pmod{120}, \\
21x + y + 40z & \equiv & 0 & \pmod{60}, \\
x + 21y + 20z & \equiv & 0 & \pmod{30}.
\end{array}$$

2.5.4. Lemma. *A 2.5.1.Lemma általánosítása: Legyen $p > 2$ prím.*
(a) Minden $(x_1, ..., x_{n+1}) \in \mathbb{Z}^{n+1}$ teljesíti a következő kongruenciák valamelyikét:

$$x_i \equiv 0 \pmod p, \qquad i = 1, ..., n+1, \tag{2.5.7}$$

$$x_i + jx_{i+1} \equiv 0 \pmod p, \qquad i = 1, ...n, \quad j = 1, ..., p-2, \tag{2.5.8}$$

$$x_1 \equiv x_{n+1} \pmod p. \tag{2.5.9}$$

(b) Mindegyik kongruenciához van olyan $x \in \mathbb{Z}^{n+1}$, amely csak azt az egy kongruenciát teljesíti ezek közül.

Bizonyítás. (a) Hasonlóan, mint az 2.5.1.Lemmánál.
(b) Legyen $x \in \mathbb{Z}^{n+1}$ a következő:
1. eset: az első $i-1$ koordinátája legyen 1, az i. koordinátája legyen p, a többi 2. Ekkor ez csak (2.5.7)-et teljesíti i-re.
2. eset: $\text{lnko}(j,p)=1$, tehát létezik j', hogy $jj' \equiv 1 \pmod{p}$. x első i koordinátája legyen $p-1$, a többi j'. Ekkor x csak (2.5.8)-at teljesíti i,j-re.
3. eset: (1,1, ...1) csak (2.5.9)-et teljesíti. □

2.5.5. Tétel. *Létezik irredundáns, teljesen n-dimenziós homogén fedőrendszer minden $n \geq 2$-re.*

Bizonyítás. Teljes indukcióval. Az indukciós feltétel: létezik olyan S_n irredundáns teljesen n-dimenziós fedőrendszer, hogy az $x_2 \equiv 0 \pmod 2$ kongruencia benne van S_n-ben, létezik r pozitív egész, hogy van egy $x_1 - ax_2 \equiv 0 \pmod{2^r}$ alakú kongruencia S_n-ben, és 2^{r+1} nem osztja egyik S_n-beli modulust sem. Ez igaz $n=2$-re, a Cochrane-Myerson-féle konstrukcióval Selfridge összetett fedőrendszeréből kapott 2-dimenziós fedőrendszer ilyen (ez volt az első példánk): $x_2 \equiv 0 \pmod 2$ és $x_1 - -6x_2 \equiv 0 \pmod{16}$ benne van a rendszerben, és egyik modulus sem osztható 32-vel. Most tegyük fel az indukciós feltételt. Legyen p olyan prím, amely nem osztója egyetlen S_n-beli modulusnak sem. Legyen $d = np - n + 2$. S_{n+1}-et úgy kapjuk S_n-ből, hogy S_n-ből elhagyjuk a 2^r modulusú kongruenciát: $x_1 - ax_2 \equiv 0 \pmod{2^r}$-t, és hozzávesszük a következő kongruenciákat:

$$x_1 + (-a + 2^{r-1+i})x_2 \equiv 0 \pmod{2^{r+i}}, \quad i = 1, ..., d, \tag{2.5.10}$$

$$\left.\begin{aligned} x_1 - ax_2 &\equiv 0 \pmod{2^{r+1}}, \\ x_1 &\equiv x_{n+1} \pmod{p}, \end{aligned}\right\} \tag{2.5.11}$$

$$\left.\begin{aligned} x_1 - ax_2 &\equiv 0 \pmod{2^{r+j+1+(i-1)(p-2)}}, \\ x_i + jx_{i+1} &\equiv 0 \pmod{p}, \quad i = 1, ..., n, \quad j = 1, ..., p-2, \end{aligned}\right\} \tag{2.5.12}$$

$$\left.\begin{aligned} x_1 - ax_2 &\equiv 0 \pmod{2^{r+np-2n+1+i}}, \\ x_i &\equiv 0 \pmod{p}, \quad i = 1, ..., n+1. \end{aligned}\right\} \tag{2.5.13}$$

Ezeknek a kongruenciáknak a modulusai: 2^k, $k = r+1, ..., r+d$ és $2^l p$, $l = = r+1, ..., r+d$ különböző számok, és mindegyik osztható 2^{r+1}-nel, tehát S_n modulusaitól is különböznek. Legyen $s = r + d$, ekkor S_{n+1}- ben van egy $x_1 - bx_2 \equiv 0 \pmod{2^s}$ alakú kongruencia, $x_2 \equiv 0 \pmod 2$ benne van S_{n+1}-ben, és egyik modulus sem osztható 2^{s+1}-nel.
Most megmutatjuk, hogy S_{n+1} fedőrendszer. $x_1 - ax_2 \equiv 0 \pmod{2^r} = (1, -a, 2^r)$ a

2-dimenziós homogén fedőrendszerekre vonatkozó jelölésünkkel. A 2.4.8.Tételt fogjuk használni. Mivel a 2 modulus a rendszerben, $(1,-a,2^r) = (1,-a+2^r,2^{r+1}) \cup \cup (1,-a,2^{r+1})$, az utóbbit tovább bontjuk: $(1,-a,2^{r+1}) = (1,-a+2^{r+1},2^{r+2}) \cap (1,--a,2^{r+2})$, és így tovább, kapjuk, hogy $(1,-a,2^r) = (1,-a,2^{r+d}) \cup \{\cup_{1\le i\le d}(1,-a++2^{r-1+i},2^{r+i})\}$. Tehát $x \in \mathbb{Z}^{n+1}$ vagy teljesíti (2.5.10)-et valamely i-re, vagy $x_1 --ax_2 \equiv 0 \pmod{2^{r+d}}$. Az utóbbi esetben a 2.5.2. Lemmát általánosítva a 2.5.4. Lemma segítségével kapjuk, hogy x teljesíti (2.5.11), (2.5.12) és (2.5.13) valamelyikét.

Már csak azt kell bizonyítanunk, hogy S_{n+1} irredundáns és teljesen n-dimenziós. Először bebizonyítjuk, hogy irredundáns. Mivel S_n irredundáns, minden kongruenciához S_n-ben létezik egy olyan $z \in \mathbb{Z}^n$, amely csak azt teljesíti. $x_1 - ax_2 \equiv 0 \pmod{2^r}$-en kívül minden S_n-beli kongruencia benne van S_{n+1}-ben is, és ha ezek közül z csak ezt az egyet teljesítette S_n-ben, akkor S_{n+1}-ben is csak ezt fogja teljesíteni, mivel $x_1 - ax_2 \equiv 0 \pmod{2^r}$-t nem teljesítí, tehát az S_{n+1}-hez újonnan hozzávett kongruenciákat sem teljesíti. Legyen $c = (c_1, \dots, c_n)$ az a vektor, amelyik csak $x_1 - ax_2 \equiv 0 \pmod{2^r}$-t teljesítette S_n-ben. Legyen $2^r m$ az S_n modulusainak legkisebb közös többszöröse, ahol m páratlan. Ekkor $c_k = (c_1 + k2^r m, c_2, \dots, c_n)$ is csak $x_1 - ax_2 \equiv 0 \pmod{2^r}$-t teljesíti S_n-ben minden k egészre. Minden $i = 1, \dots, d$-re van olyan k, hogy c_k teljesíti $x_1 + (-a + 2^{r-1+i})x_2 \equiv 0 \pmod{2^{r+i}}$-t, ugyanis ha ebbe beírjuk c_k-t és osztunk 2^r-nel, akkor a következő kongruenciát kapjuk:

$$mk \equiv 2^{i-1}c_2 - \frac{c_1 - ac_2}{2^r} \pmod{2^i}. \tag{2.5.14}$$

Legyen $u_k \equiv c_k \pmod{2^{r+d}m}$ és $u_k \equiv (1,1,...,1,0) \pmod{p}$. Ekkor u_k csak $x_1 + + (-a + 2^{r-1+i})x_2 \equiv 0 \pmod{2^{r+i}}$-t teljesíti S_{n+1}-ben. Ugyanis tegyük fel, hogy u_k teljesíti (2.5.10)-t egy másik i-re, mondjuk $i = t$-re. Ekkor

$$mk \equiv 2^{t-1}c_2 - \frac{c_1 - ac_2}{2^r} \pmod{2^t},$$

és ebből kapjuk, hogy $2^{i-1}c_2 \equiv 2^{t-1}c_2 \pmod{\min\{t,i\}}$, és ha $t \neq i$, akkor c_2-nek oszthatónak kell lennie 2-vel, de ez nem lehetséges, mivel c nem teljesíti $x_2 \equiv 0 \pmod 2$-t.

A modulo p tett feltétel miatt u_k nyilván nem teljesíti (2.5.11)-et és (2.5.12)-t. Most tegyük fel, hogy u_k teljesíti (2.5.13)-at. Mivel csak az utolsó koordináta osztható p-vel, ez csak úgy lehet, ha $i = n + 1$, vagyis c_k teljesíti $x_1 - ax_2 \equiv 0 \pmod{2^{r+d}}$-t. Ekkor

$$mk \equiv -\frac{c_1 - ac_2}{2^r} \pmod{2^d},$$

és mivel $i \le d$ és (2.5.14) teljesül, kapjuk, hogy $0 \equiv 2^{i-1}c_2 \pmod{2^i}$. Ez pedig csak úgy lehetne, ha a kettő osztaná c_2-t, de ez nem teljesül.

Tehát minden (2.5.10)-beli kongruenciához mutattunk egy olyan vektort, amely csak azt az egyet teljesíti S_{n+1}-ben.

Most minden (2.5.11), (2.5.12) és (2.5.13)-beli kongruenciához is mutatunk egy olyan vektort, amely csak azt az egyet teljesíti S_{n+1}-ben. Legyen $v \in \mathbb{Z}^{n+1}$ olyan vektor, amely pontosan egyet teljesít a 2.5.4. Lemma-beli kongruenciák közül. Legyen k olyan, hogy c_k teljesíti $x_1 - ax_2 \equiv 0 \pmod{2^{r+d}}$-t. Legyen $u \equiv v \pmod{p}$ és $u \equiv c_k \pmod{2^{r+d}m}$. Ekkor u pontosan egyet teljesít az S_{n+1}-beli kongruenciák közül, és minden (2.5.11), (2.5.12) vagy (2.5.13)-beli kongruenciához van ilyen u.

Ezzel bebizonyítottuk, hogy S_{n+1} irredundáns. Már csak azt kell belátni, hogy teljesen $n+1$-dimenziós.

Tegyük fel, hogy S_{n+1} egy q-dimenziós T fedőrendszer képe. Ekkor T-ben vannak a következő kongruenciák alkalmas b_{ij} együtthatókkal:

$$b_{i1}y_1 + ... + b_{iq}y_q \equiv 0 \pmod{2^{r+np-2n+1+i}}, \quad i = 1, ..., n+1,$$

és $y_j = \sum_{t=1}^{n+1} f_{tj}x_t$ helyettesítéssel ezek a (2.5.13)-beli kongruenciákba mennek át. Ekkor

$$0 \equiv \sum_{j=1}^{q} b_{ij}y_j \equiv \sum_{j=1}^{q} \big(b_{ij} \sum_{t=1}^{n+1} f_{tj}x_t\big) \equiv \sum_{t=1}^{n+1} \big(\sum_{j=1}^{q} b_{ij}f_{tj}\big)x_t \pmod{2^{r+np-2n+1+i}},$$

amiből kapjuk, hogy

$$\sum_{t=1}^{n+1} \big(\sum_{j=1}^{q} b_{ij}f_{tj}\big)x_t \equiv x_i \pmod{p}, \quad i = 1, ..., n+1.$$

Tehát, ha $B = (b_{ij})$ és $F = (f_{jt})$ mátrixok, I az $(n+1) \times (n+1)$-es egységmátrix, akkor $BF^T \equiv I \pmod{p}$, de B és F rangja legfeljebb q, tehát $n+1 \leq q$ vagyis S_{n+1} teljesen $n+1$-dimenziós. □

2.5.6. Megjegyzés. *Jin és Myerson cikkében volt egy kis hiba, (2.5.12) helyett a következő kongruencia állt:*

$$x_1 - ax_2 \equiv 0 \pmod{2^{r+j+(i-1)(p-2)}} \wedge x_i + jx_{i+1} \equiv 0 \pmod{p},$$
$$i = 1, ..., n, \quad j = 2, ..., p-1.$$

Ez azért nem jó, mert például páratlan n esetén legyen $w \in \mathbb{Z}^{n+1}$ olyan vektor, hogy w teljesítse $x_1 - ax_2 \equiv 0 \pmod{2^{r+d}}$-t és legyen $w \equiv (1, -1, 1, -1, ..., 1, -1) \pmod{p}$. Ekkor w nem teljesíti (2.5.11), (2.5.12) és (2.5.13) egyikét sem.

2.5.7. Megjegyzés. *S_{n+1} konstruálásakor p választására végtelen sok lehetőség volt, és különböző p-kre különböző, irredundáns $n+1$-dimenziós fedőrendszereket kapunk,*

tehát végtelen sok (teljesen) n-dimenziós homogén fedőrendszer van minden $n > 2$-re.

2.6. Nyitott kérdések

Rengeteg nyitott kérdés van fedőrendszerekkel kapcsolatban, lásd például [9]-ben. Most mi is felvetünk néhány kérdést, főleg többdimenziós fedőrendszerekkel kapcsolatban:

Létezik-e összetett 2-dimenziós homogén fedőrendszer? És ha igen, van-e végtelen sok különböző?

Tudjuk, hogy az egydimenziós fedőrendszerek modulusainak reciprokösszege nagyobb, mint 1. A 2.2.6. Tételből következik, hogy ez igaz kétdimenziós homogén fedőrendszerekre is. Két dimenzióban tudjuk-e ezt javítani? Azaz létezik-e olyan $c > 1$ konstans, hogy minden kétdimenziós homogén fedőrendszer modulusainak reciprokösszege nagyobb, mint c?

Egy dimenzióban tudunk válaszolni arra a kérdésre, hogy minden $N > 3$-ra van-e olyan fedőrendszer, amelynek modulusait nem osztják az N-nél kisebb páratlan prímek. Ugyanis, ha 2 $\uparrow$-nál p-t N-nél nagyobbra választjuk, egy ilyen fedőrendszert kapunk. Tudunk-e ilyet mutatni a kétdimenziós homogén fedőrendszerek között is? Ha nem, mi az a legnagyobb N, amelyre van olyan kétdimenziós homogén fedőrendszer, amelynek modulusai nem oszthatók az N-nél kisebb páratlan prímekkel? A kérdés ekvivalens ugyanezzel a kérdéssel összetett egydimenziós fedőrendszerekre.

Hivatkozások

[1] P. Erdős, On integers of the form $2^k + p$ and some related problems, Summa Brasil. Math. 2 (1950) 113–123.

[2] P. P. Nielsen, A covering system whose smallest modulus is 40, Journal of Number Theory 129 (2009) 640-666.

[3] R. Freud, E. Gyarmati, Számelmélet, Nemzeti Tankönyvkiadó (2006) 536-538.

[4] T. Cochrane, G. Myerson, Covering congruences in higher dimensions, Rocky Mountain J. Math. 26 (1996) 77–81.

[5] A. Schinzel, On homogeneous covering congruences, Rocky Mountain J. Math. 27 (1997) 335–342.

[6] R. J. Simpson, Covering systems of homogeneous congruences, Rocky Mountain J. Math. 28 (1998) 1125–1133.

[7] B. Jin, G. Myerson, Homogeneous covering congruences and subgroup covers, Journal of Number Theory 110 (2005) 120–135.

[8] S. Jenkin, J. Simpson, Composite covering systems of minimum cardinality, Integers 3 (2003) Paper A13, 11 p., electronic only-Paper A13, 11 p., electronic only. <http://eudml.org/doc/123108>

[9] R. K. Guy, Unsolved problems in number theory, Second edition, Springer-Verlag (1994)