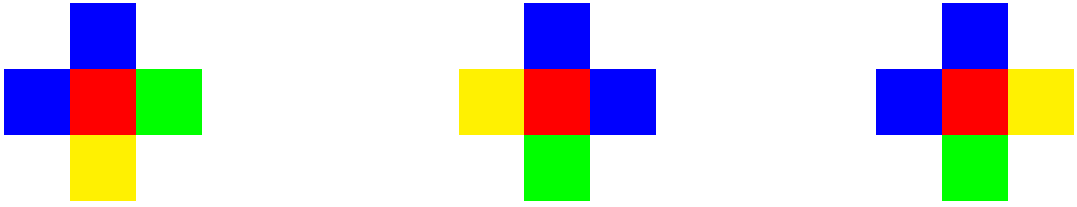
Algebra és számelmélet előadás

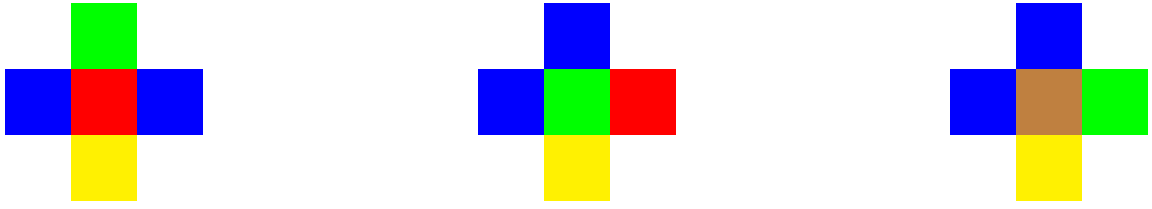
Waldhauser Tamás
2016. december 1.

Tizedik házi feladat az előadásra

Hányféleképpen lehet kiszínezni az X-pentominót n színnel, ha a forgatással vagy tükrözéssel egymásba vihető színezéseket nem tekintjük különbözőnek? (Lehet $n > 5$ is, mert nem kötelező az összes színt felhasználni.) Például az alábbi három színezés egyformának számít



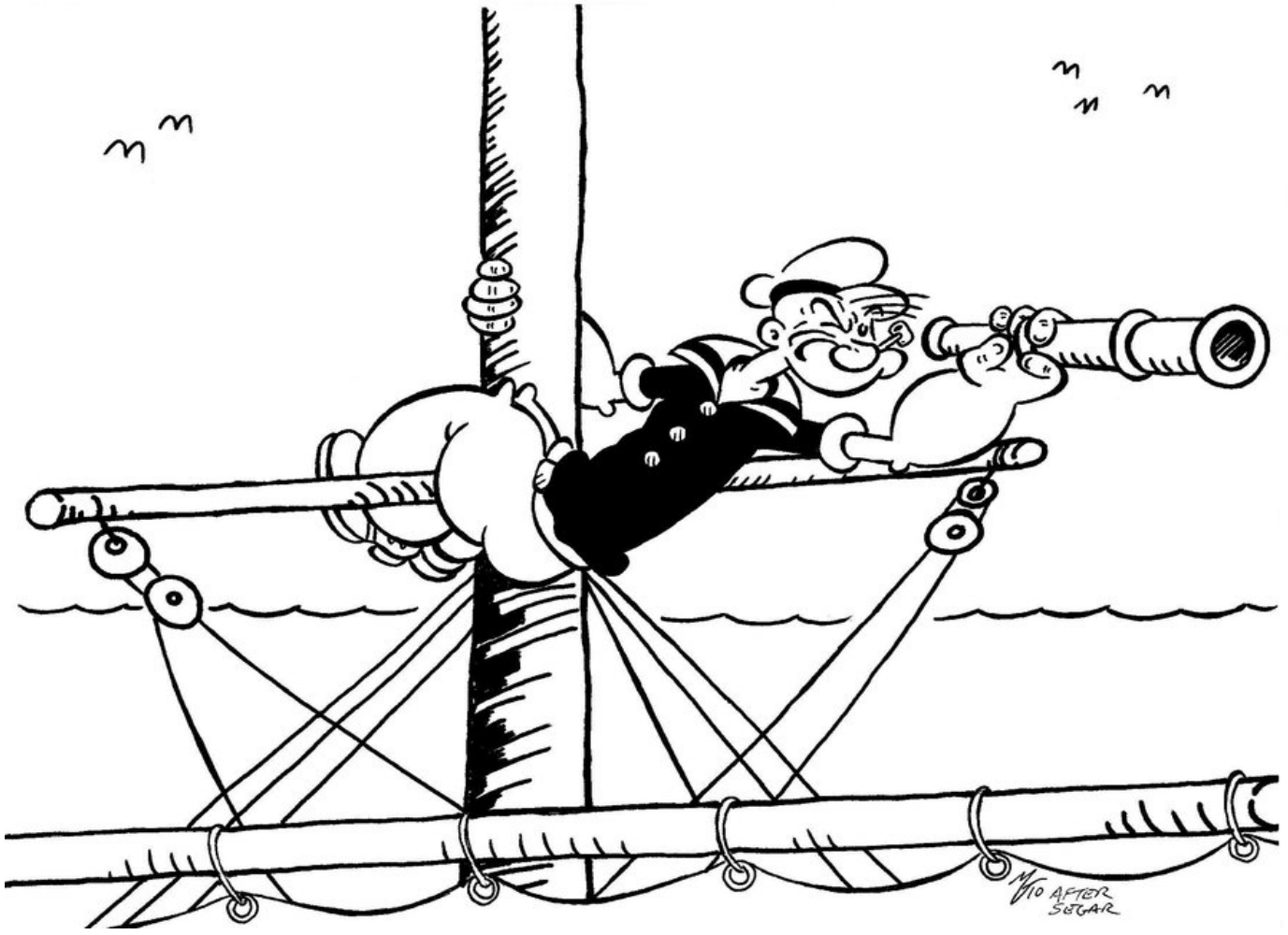
de a következő színezések már különböznek a fentiektől (és egymástól is):



Eredmény:

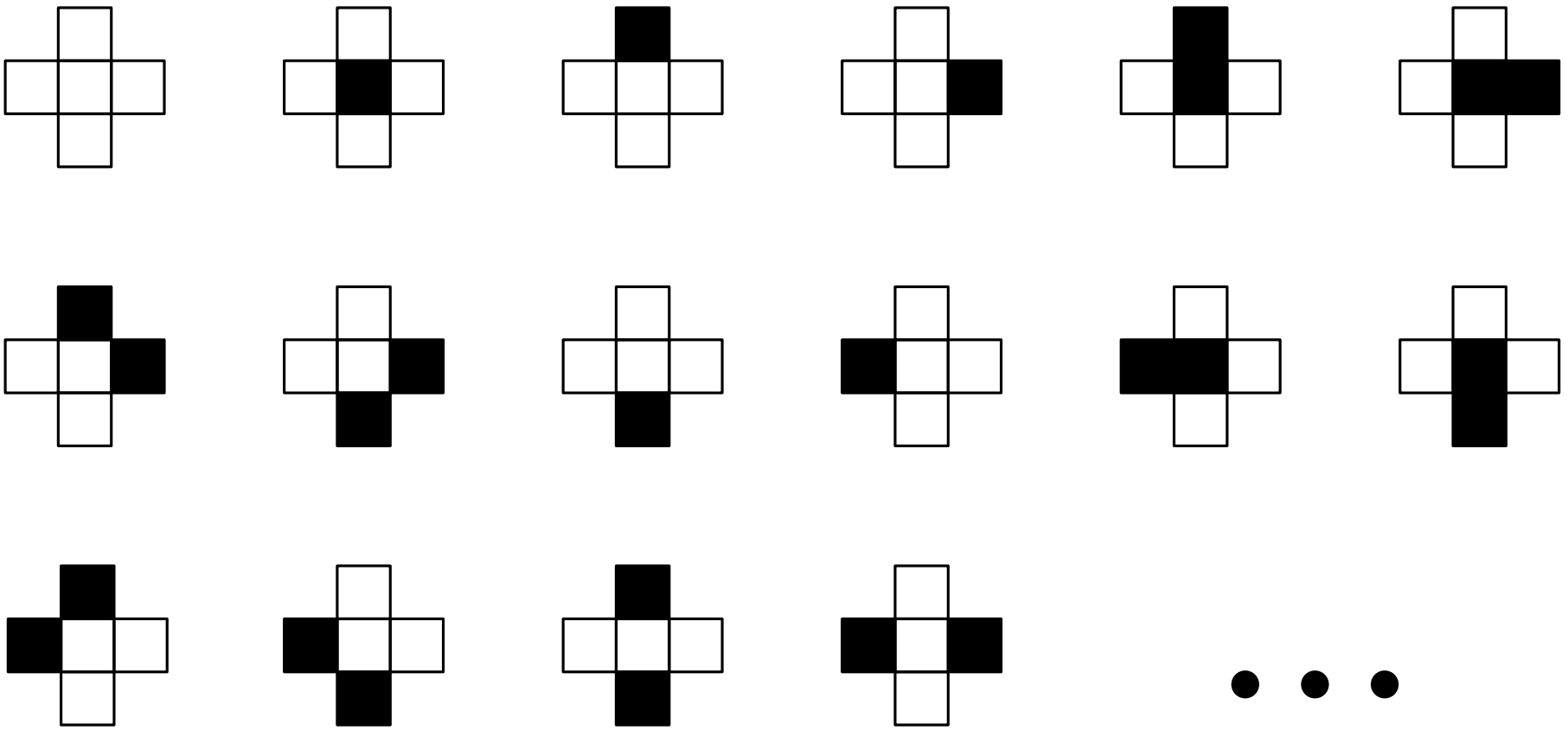
$$\binom{n}{1} \cdot 1 + \binom{n}{2} \cdot 10 + \binom{n}{3} \cdot 30 + \binom{n}{4} \cdot 36 + \binom{n}{5} \cdot 15 = \frac{1}{8}n^5 + \frac{1}{4}n^4 + \frac{3}{8}n^3 + \frac{1}{4}n^2$$

Kitekintés: Pólya–Redfield-módszer



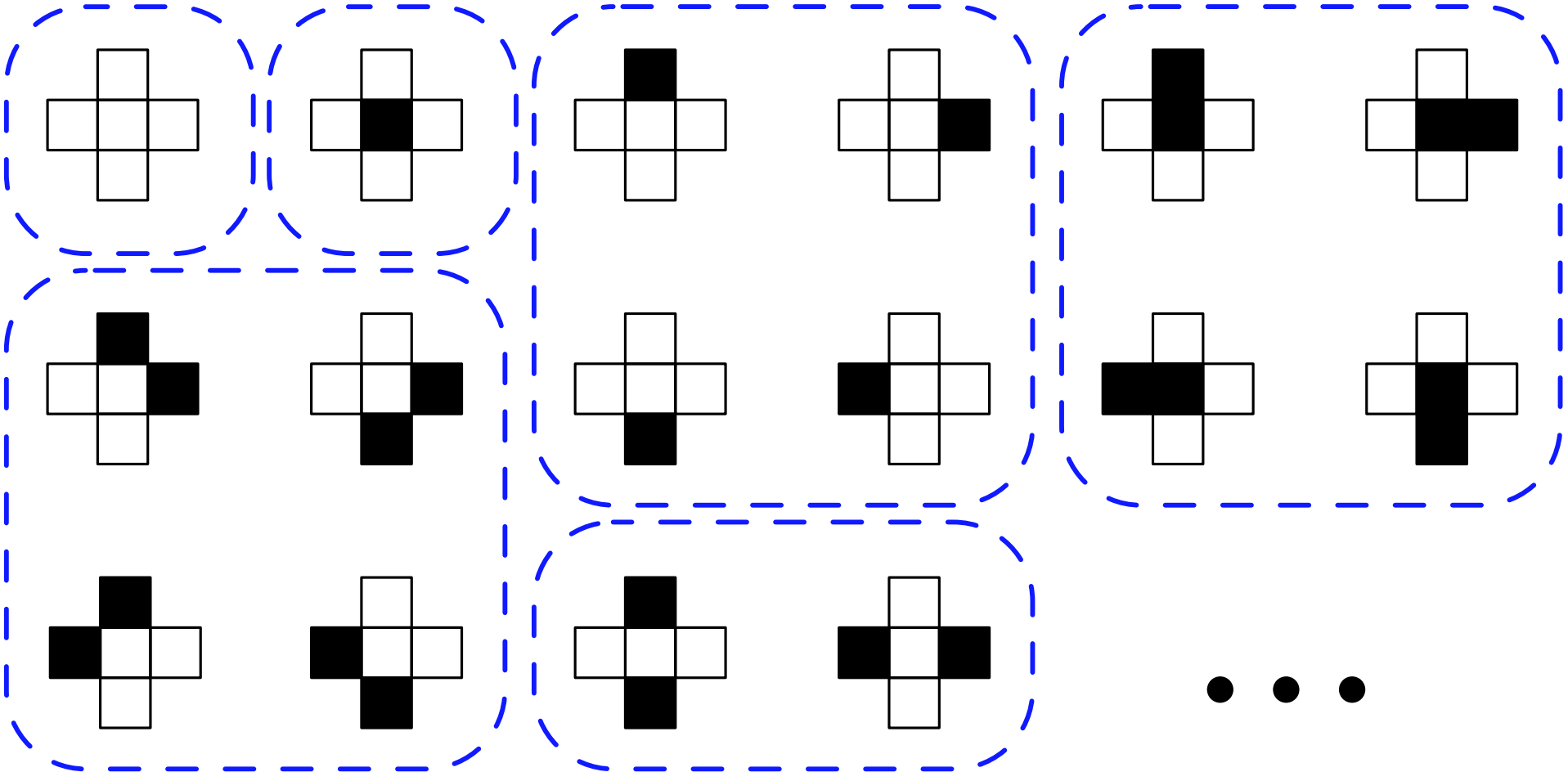
Az összes színezés

Legyen Sz az összes színezések halmaza. Nyilván $|Sz| = n^5$. Például $n = 2$ esetén:



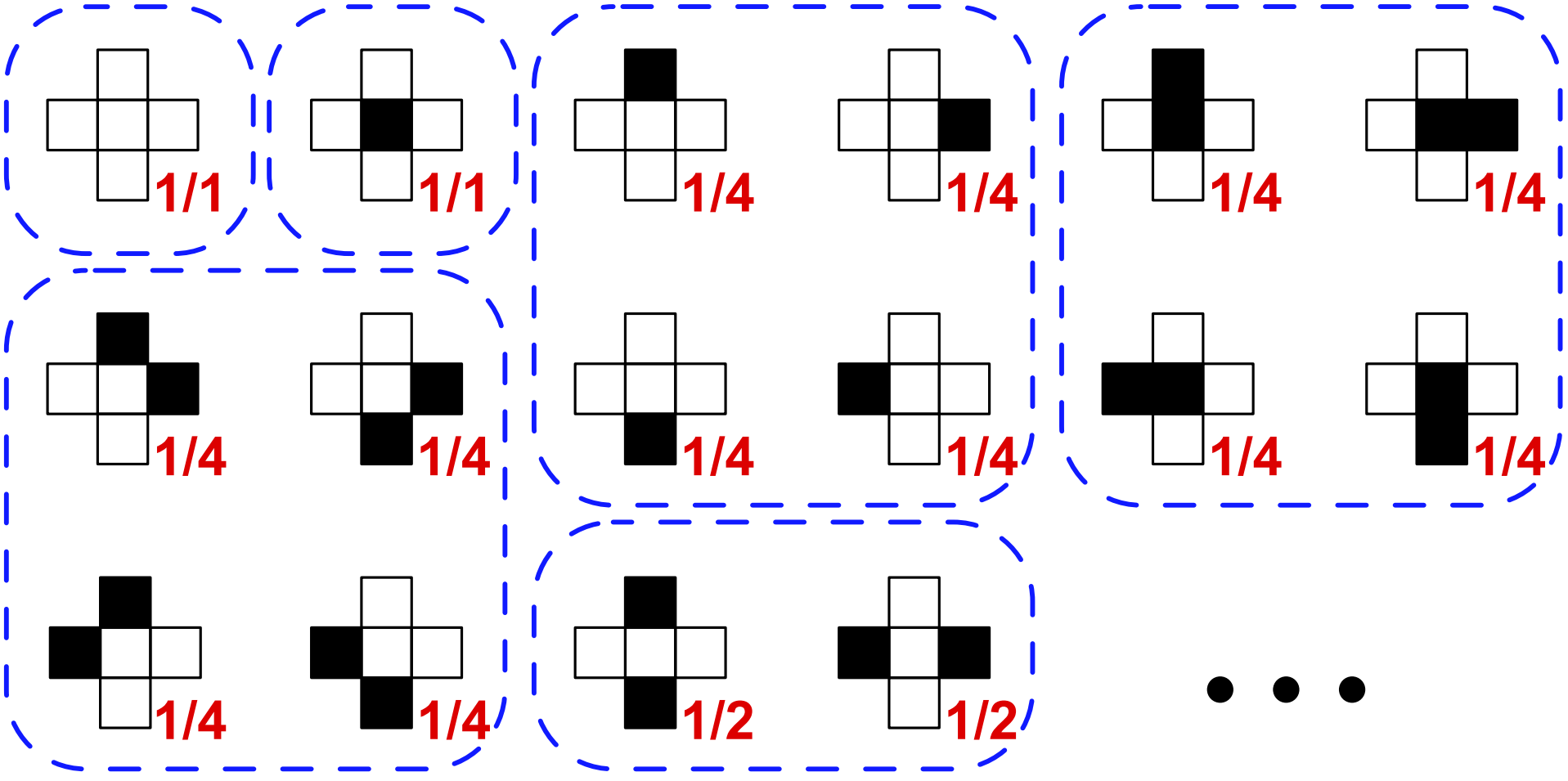
A színezések osztályozása

Legyen Sz az összes színezések halmaza. Nyilván $|Sz| = n^5$. Például $n = 2$ esetén:



Piros számok

Legyen Sz az összes színezések halmaza. Nyilván $|Sz| = n^5$. Például $n = 2$ esetén:



Színezés szimmetria erejéig

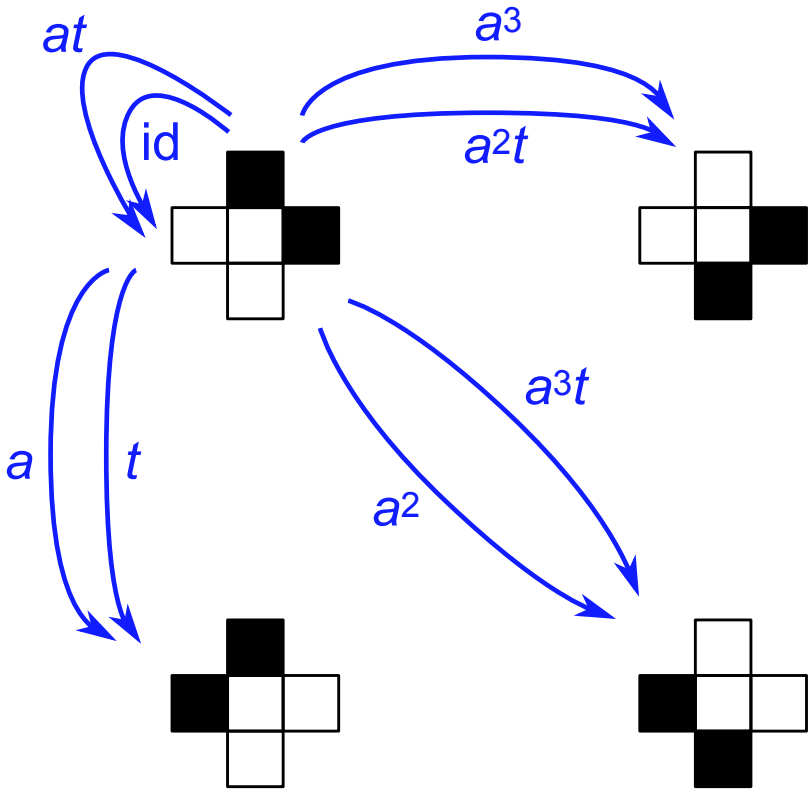
Legyen Sz az összes színezések halmaza, és definiáljuk Sz-en az alábbi ekvivalenciarelációt:

$$sz_1 \sim sz_2 \iff \exists g \in D_4 : sz_1\, g = sz_2.$$

Feladatunk az ekvivalenciaosztályok (pályák) számának meghatározása.
Mivel minden ekvivalenciaosztályon belül 1 a piros számok összege,

$$|Sz| \,/\, \sim \;\; = \sum_{Sz} \text{piros számok}$$

Csoportelmélet!



Stabilizátor: $\{\mathrm{id}, at\} \leq D_4$.

Mellékosztályok: $\{\mathrm{id}, at\}$,
$\{a, t\}$,
$\{a^2, a^3 t\}$,
$\{a^3, a^2 t\}$.

Egy rögzített $sz \in Sz$ színezést a saját ekvivalenciaosztályának minden tagjába ugyanannyi D_4-beli elem visz el, (mert $sz\, g_1 = sz\, g_2$ akkor és csak akkor, ha g_1 és g_2 ugyanabba a jobb oldali mellékosztályba tartoznak sz stabilizátora szerint).

Tehát egy sz színezéshez írt piros szám nem más, mint a stabilizátora indexének reciproka:

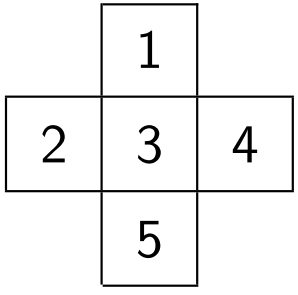
$$\frac{|\{g \in D_4 : sz\, g = sz\}|}{|D_4|} = \mathrm{P}\left(sz\, g = sz\right).$$

Valószínűségszámítás!

$$
\begin{aligned}
|Sz| \,/\sim \quad &= \quad \sum_{Sz} \text{piros számok} \\
&= \quad \sum_{Sz} \mathrm{P}\left(sz\, g = sz\right) \\
&= \quad \mathrm{E}\left(g \text{ fixpontjainak száma}\right) \\
&= \quad \text{átlagos fixpontszám} \\
&= \quad \frac{1}{|D_4|} \cdot \sum_{D_4} \left(g \text{ fixpontjainak száma}\right)
\end{aligned}
$$

Kombinatorika!

Tetszőleges $sz \in Sz$ és $g \in D_4$ esetén $sz\,g = sz$ akkor és csak akkor teljesül, ha egyszínűek azok a négyzetek, amelyek egymásba mennek a g transzformáció végrehajtása során. Ha g-nek, mint az öt kis négyzet permutációjának, c ciklusa van, akkor az ilyen színezések száma n^c.



D_4 eleme	S_5 eleme	c	fixpontok száma (Sz-ben)
id	(1) (2) (3) (4) (5)	5	n^5
a	(1254) (3)	2	n^2
a^2	(15) (24) (3)	3	n^3
a^3	(1452) (3)	2	n^2
t	(1) (24) (3) (5)	4	n^4
at	(14) (25) (3)	3	n^3
a^2t	(15) (2) (3) (4)	4	n^4
a^3t	(12) (3) (45)	3	n^3

$$|Sz| \,/\, \sim \;=\; \text{átlagos fixpontszám} \;=\; \frac{1}{8} \cdot \left(n^5 + 2n^4 + 3n^3 + 2n^2\right)$$

Pólya–Redfield-módszer

Legyen $G \leq S_A$ egy permutációcsoport. Tetszőleges $g \in G$ esetén jelölje $c(g)$ a g permutáció ciklusainak számát (beleértve az egy hosszúságú ciklusokat is). Az

$$f = \sum_{g \in G} x^{c(g)} \in \mathbb{Z}[x]$$

polinomot a G csoport ciklusszámláló polinomjának nevezzük (majdnem).

Tétel (John Howard Redfield, 1927 és Pólya György, 1937).

Az A halmaz n színnel történő színezéseinek száma „modulo G" éppen $f(n)$.

Példa.

Láttuk, hogy a kocka forgáscsoportja 24-elemű. Ha a forgatásokat, mint a lapok permutációit tekintjük (azaz S_6 részcsoportjaként), akkor a ciklusszámláló polinom:

$$\frac{1}{24} \cdot \left(x^6 + 3x^4 + 12x^3 + 8x^2\right).$$

Tehát a kocka lapjait ennyiféleképpen lehet x színnel kiszínezni, ha a forgatásokkal egymásba vihető színezéseket nem tekintjük különbözőnek.

Az Euler-féle φ függvény

Leonhard Euler

(1707, Bázel – 1783, Szentpétervár)

Euler–Fermat-tétel

5.5. Tétel (Euler–Fermat-tétel).

Ha az a egész szám relatív prím az m modulushoz, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Bizonyítás.

Alkalmazzuk Lagrange tételét (pontosabban a 4.57. Következmény harmadik állítását) a $\mathbb{Z}_m^*$ csoportra. □

5.6. Következmény (kis Fermat-tétel).

Ha p prímszám és a nem osztható p-vel, akkor $a^{p-1} \equiv 1 \pmod{p}$.

Bizonyítás.

Ha p prím, akkor $\varphi(p) = p - 1$. □

5.7. Következmény.

Ha $a \in \mathbb{Z}$ relatív prím az m modulushoz és $k, \ell \in \mathbb{Z}$, akkor

$$k \equiv \ell \pmod{\varphi(m)} \Longrightarrow a^k \equiv a^\ell \pmod{m}.$$

Bizonyítás.

Ha $k \equiv \ell \pmod{\varphi(m)}$, akkor $\exists t \in \mathbb{Z}\colon k = \ell + t \cdot \varphi(m)$, és így

$$a^k \equiv a^{\ell + t\cdot\varphi(m)} \equiv a^\ell \cdot \left(a^{\varphi(m)}\right)^t \equiv a^\ell \cdot 1^{\varphi(m)} \equiv a^\ell \pmod{m}.$$ □

Házi feladat a gyakorlatra

37. feladat. Számítsa ki az alábbi hatványok maradékait a megadott modulusra nézve.

(a) $2014^{2014} \equiv ? \pmod 7$ $\quad 2014^{2014} \equiv 5^4 \equiv 2 \pmod 7$

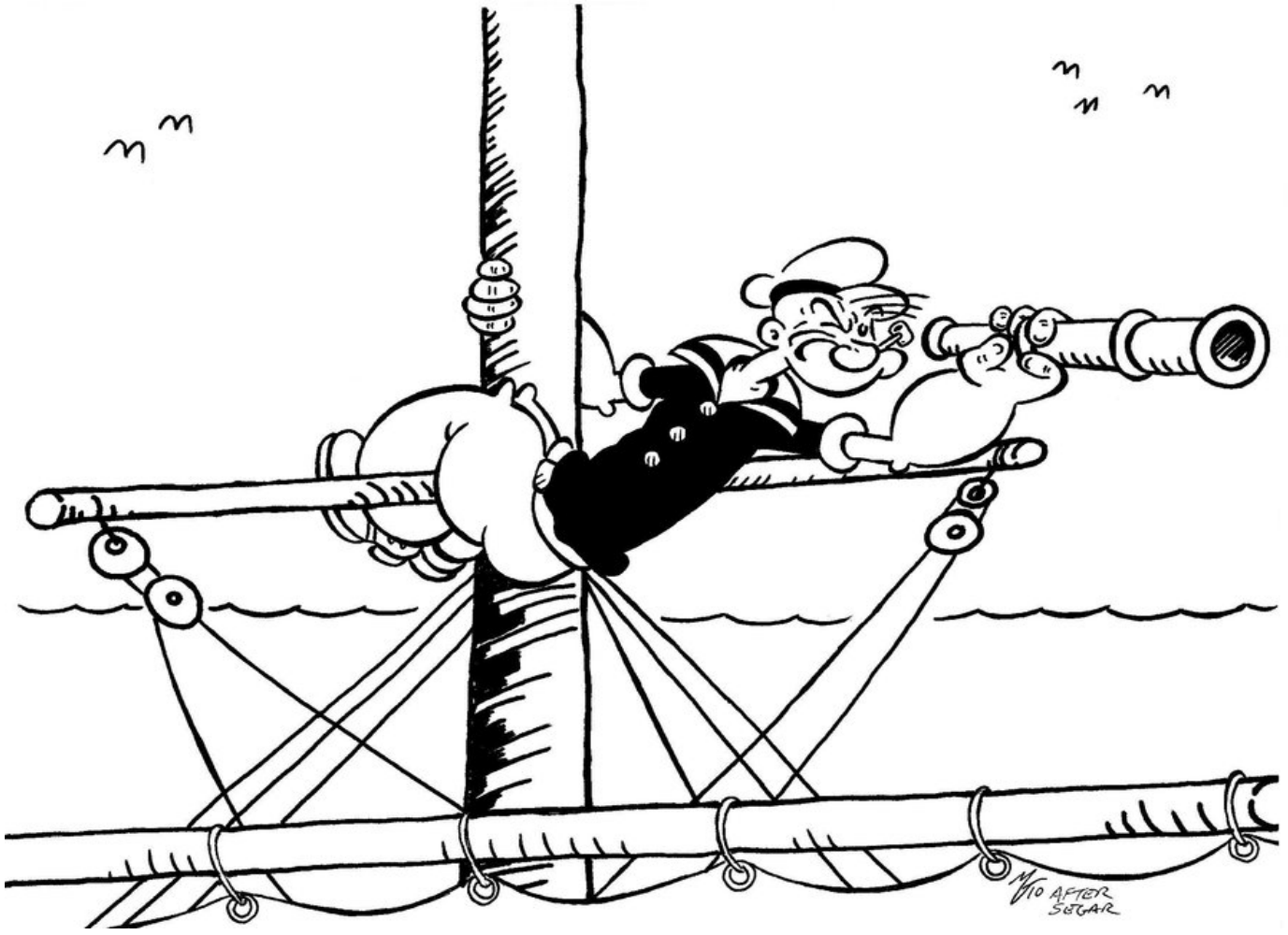
(b) $27^{159} \equiv ? \pmod{40}$ $\quad 27^{159} \equiv 27^{-1} \equiv 3 \pmod{40}$

(c) $4447^{2018} \equiv ? \pmod{44}$

(d) $303^{4039} \equiv ? \pmod{100}$

(e) $2019^{2019} \equiv ? \pmod{11}$

Kitekintés: titkosírások



Nyilvános kulcsú titkosírások

Egy ü üzenetet titkosítunk a T titkosítófüggvénnyel.

- nyilvános rész: T és $T(\text{ü})$
- titkos rész: T^{-1} (és persze ü)

Olyan T függvényt kell választani, amelynek az inverzét nehéz kiszámítani.

Ötlet: könnyű összeszorozni két nagy (prím)számot, de nehéz (prím)tényezőkre bontani a szorzatot. (Jevons, 1874)

Konkrét megvalósítás: RSA (Cocks, 1973, és Rivest-Shamir-Adleman, 1977)

Az RSA-eljárás

Legyen $m = pq$, ahol p és q nagy prímszámok, és legyenek e, d olyan természetes számok, hogy $ed \equiv 1 \pmod{\varphi(m)}$. Ekkor az alábbi két függvény egymás inverze:

$$T : \mathbb{Z}_m \to \mathbb{Z}_m,\ \overline{x} \mapsto \overline{x}^e;$$
$$T^{-1} : \mathbb{Z}_m \to \mathbb{Z}_m,\ \overline{x} \mapsto \overline{x}^d.$$

Valóban, ha $x \perp m$, akkor az Euler–Fermat-tétel szerint x kitevője csak modulo $\varphi(m)$ „számít", azaz

$$(x^d)^e \equiv (x^e)^d \equiv x^{ed} \equiv x^1 \pmod{m}.$$

(HF: és ha x nem relatív prím m-hez?)

Ha ismert p és q, akkor $\varphi(m) = (p-1)(q-1)$ könnyen kiszámítható, és adott e kitevőhöz könnyen lehet megfelelő d párt találni (hogyan?).

Ha viszont csak m és e (azaz a T függvény) ismert, akkor nehéz(??) kiszámolni a d kitevőt (azaz a T^{-1} függvényt).

Az RSA-eljárás

Alice és Bob szeretne egymással üzenetet váltani. Alice választ p_A, q_A nagy prímeket és e_A, d_A kitevőket úgy, hogy $e_A \cdot d_A \equiv 1 \pmod{\varphi(p_A \cdot q_A)}$.

- nyilvános rész: $m_A = p_A q_A$ modulus, e_A nyilvános kitevő
- titkos rész: p_A, q_A prímek, d_A titkos kitevő

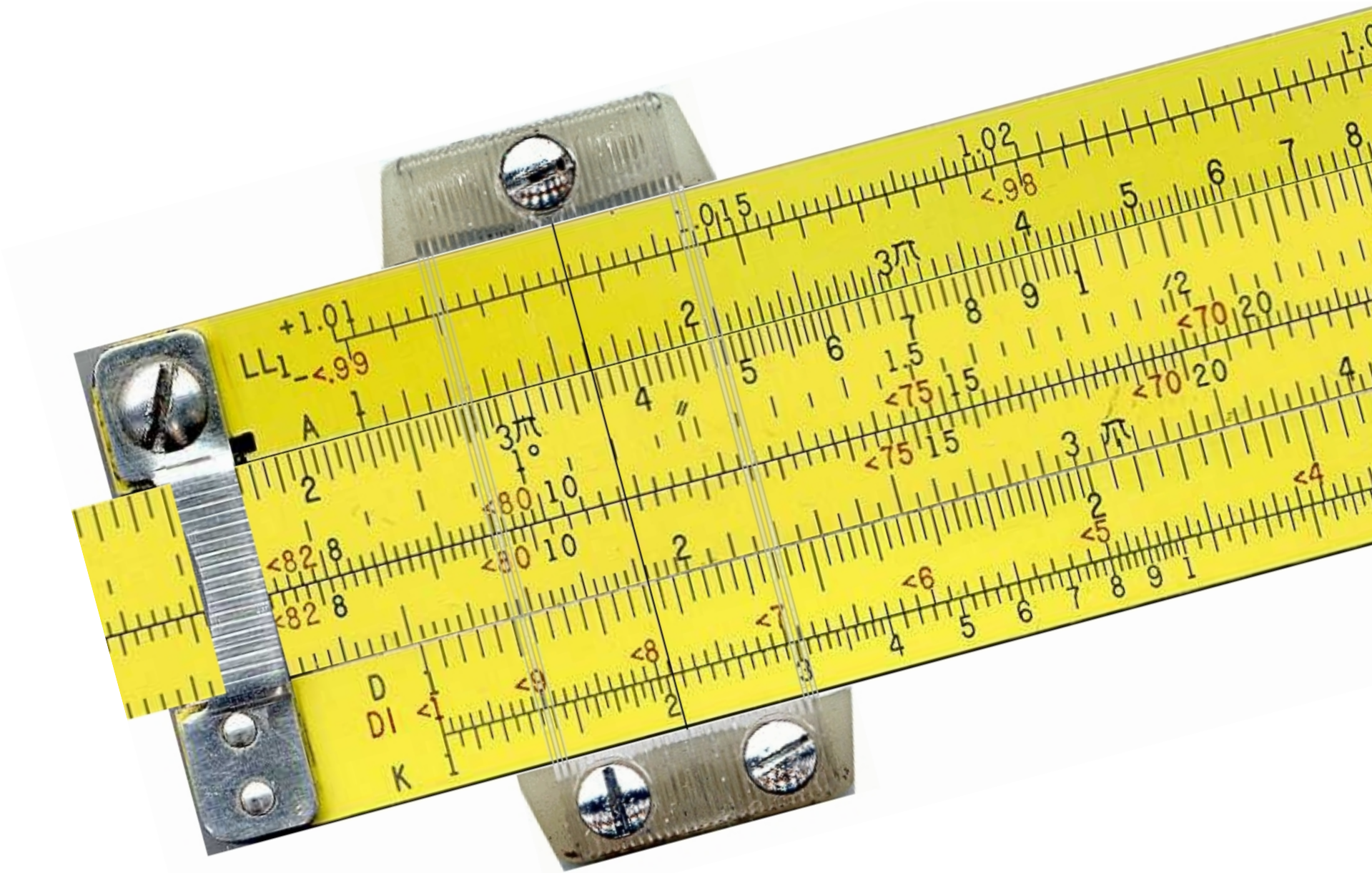
Ha Bob az ü üzenetet akarja küldeni Alice-nek (tfh. $1 \leq$ü$\leq m_A$), akkor az ^{e_A} hatvány modulo m_A maradékát küldi el, és azt Alice dekódolja a titkos kitevőjével: $(\text{ü}^{e_A})^{d_A} \equiv$ü $\pmod{m_A}$.

Bob (és mindenki, aki részt akar venni a kommunikációban), szintén generál magának p_B, q_B prímeket és e_B, d_B kitevőket, és közli Alice-szel (vagy akár az egész világgal) az $m_B = p_B q_B$ modulust és e_B nyilvános kitevőt.

Ha Alice (vagy bárki más) üzenni akar Bobnak, akkor azt az $\text{ü}^{e_B} \bmod m_B$ titkosítással kódolja, amit csak Bob tud dekódolni (remélhetőleg).

Mindez használható az üzenet küldőjének azonosítására (hiteles aláírás), sőt telefonon keresztül történő pénzfeldobásra is!

Rend, primitív gyök, index



Primitív gyök

5.8. Definíció.

Legyen $a \in \mathbb{Z}$ relatív prím az m modulushoz. Ekkor az a szám *modulo m rendjén* az $\overline{a} \in \mathbb{Z}_m^*$ maradékosztály rendjét értjük (a $\mathbb{Z}_m^*$ multiplikatív csoportban). Jelölés: $o_m(a)$.

5.9. Állítás.

Tetszőleges $a \in \mathbb{Z}$ és $m \geq 2$ természetes szám esetén $a \perp m \implies o_m(a) \mid \varphi(m)$.

5.10. Definíció.

Azt mondjuk, hogy a g egész szám *primitív gyök* modulo m, ha rendje éppen $\varphi(m)$.

5.11. Állítás.

A g egész szám akkor és csak akkor primitív gyök modulo m, ha az összes mod m redukált maradékosztály megkapható $\overline{g}$ hatványaként.

Bizonyítás.

Mint a 4.39. Tétel bizonyításában: $[\overline{g}] \subseteq \mathbb{Z}_m^*$, ezért a két halmaz akkor és csak akkor egyezik meg, ha ugyanannyi elemük van:

$$[\overline{g}] = \mathbb{Z}_m^* \iff |[\overline{g}]| = |\mathbb{Z}_m^*| \iff o_m(g) = \varphi(m).$$

□

Házi feladat a gyakorlatra

38. feladat. Keressen primitív gyököt az m modulusra nézve.

(a) $m = 26$ $\quad 7, 11, 15, 19$

(b) $m = 35$

Nincs, mert $a \perp 35$ esetén

$$a^{\varphi(5)} = a^4 \equiv 1 \pmod 5 \text{ és } a^{\varphi(7)} = a^6 \equiv 1 \pmod 7,$$

és ebből az következik, hogy $a^{12} \equiv 1 \pmod{35}$, azaz

$$o_m(a) \leq 12 < \varphi(35) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24.$$

(c) $m = 17$

(d) $m = 22$

(e) $m = 19$

Index

5.12. Tétel.

Akkor és csak akkor létezik primitív gyök az m modulushoz (vagyis a $\mathbb{Z}_m^*$ csoport akkor és csak akkor ciklikus), ha $m = 2$, 4, p^α, $2p^\alpha$, ahol p páratlan prímszám és $\alpha \in \mathbb{N}$. Ezekben az esetekben a mod m primitív gyökök száma $\varphi(\varphi(m))$.

5.13. Definíció.

Tegyük fel, hogy g primitív gyök az m modulushoz. Az a egész szám *indexén* (az m modulusra és a g primitív gyökre nézve) olyan i kitevőt értünk, amelyre $g^i \equiv a \pmod{m}$. Jelölés: $\operatorname{ind}_g a$ (a modulus többnyire világos a szövegkörnyezetből).

5.14. Megjegyzés.

Világos, hogy ha a és m nem relatív prím, akkor $\operatorname{ind}_g a$ nem értelmezett (ugyanis g^i mindig relatív prím m-hez).
Ha viszont a és m relatív prím, akkor az 5.11. Állítás szerint a előáll g hatványaként modulo m, tehát ekkor $\operatorname{ind}_g a$ értelmezett.
A 4.33. Állításból következik, hogy az index modulo $\varphi(m)$ egyértelműen meghatározott.

Index

5.15. Tétel.

Legyen g primitív gyök modulo m, legyen k tetszőleges egész szám, a és b pedig relatív prímek m-hez. Ekkor érvényesek az alábbi azonosságok:

(1) $\operatorname{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$;

(2) $\operatorname{ind}_g (ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}$;

(3) $\operatorname{ind}_g a^k \equiv k \cdot \operatorname{ind}_g a \pmod{\varphi(m)}$;

(4) $\operatorname{ind}_g \left(ab^{-1}\right) \equiv \operatorname{ind}_g a - \operatorname{ind}_g b \pmod{\varphi(m)}$.

Bizonyítás.

Hasonló a logaritmus azonosságaihoz. Csak (4)-et bizonyítjuk, a többi HF.

Legyen $i = \operatorname{ind}_g a$ és $j = \operatorname{ind}_g b$, ekkor $a \equiv g^i \pmod{m}$ és $b \equiv g^j \pmod{m}$.

Ebből következik, hogy $g^{i-j} \equiv g^i \cdot \left(g^j\right)^{-1} \equiv a \cdot b^{-1} \pmod{m}$.

Az index definíciója szerint ez azt jelenti, hogy $a \cdot b^{-1}$ indexe $i - j$. □

Házi feladat a gyakorlatra

39. feladat. Készítsen indextáblázatot, és oldja meg a segítségével a kongruenciát.

(a) $x^9 \equiv 8 \pmod{13}$

indextáblázat a $g = 2$ primitív gyökhöz:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_g a$	0	1	4	2	9	5	11	3	8	10	7	6

A kongruencia megoldásai: $x \equiv 7, 8, 11 \pmod{13}$.

(b) $11x^8 \equiv 5 \pmod{13}$

Nincs megoldása.

(c) $3x^4 \equiv 4 \pmod{11}$

(d) $5x^6 \equiv 3 \pmod{11}$

(e) $10x^5 \equiv 1 \pmod{11}$

Hatványmaradékok

5.16. Definíció.

Azt mondjuk, hogy az a egész szám *n-edik hatványmaradék* modulo m, ha az $x^n \equiv a \pmod{m}$ kongruenciának van megoldása.

5.17. Tétel.

Legyen g primitív gyök modulo m, és legyen a relatív prím m-hez. Ekkor a pontosan akkor n-edik hatványmaradék modulo m, ha $\operatorname{lnko}(n, \varphi(m)) \mid \operatorname{ind}_g a$.

Bizonyítás.

Az $x^n \equiv a \pmod{m}$ kongruencia megoldását kereshetjük $x \equiv g^i$ alakban (miért?):

$$x^n \equiv a \pmod{m} \iff g^{n \cdot i} \equiv g^{\operatorname{ind}_g a} \pmod{m} \iff n \cdot i \equiv \operatorname{ind}_g a \pmod{\varphi(m)}.$$

Ez utóbbi egy lineáris kongruencia (az i ismeretlenre nézve), amelynek akkor és csak akkor van megoldása, ha $\operatorname{lnko}(n, \varphi(m)) \mid \operatorname{ind}_g a$. □

Négyzetes maradékok, Legendre-szimbólum

Adrien-Marie Legendre

(1752, Párizs – 1833, Párizs)

Legendre-szimbólum

5.18. Definíció.

Az a egész számot *négyzetes maradéknak* nevezzük modulo m, ha az $x^2 \equiv a \pmod{m}$ kongruenciának van megoldása. Ellenkező esetben azt mondjuk, hogy a *négyzetes nemmaradék* modulo m.

5.19. Tétel.

Legyen p páratlan prímszám és g primitív gyök modulo p. Ekkor $a \in \mathbb{Z}$ pontosan akkor négyzetes maradék modulo p, ha $p \mid a$ vagy $\operatorname{ind}_g a$ páros.

Bizonyítás.

Ha $p \mid a$, akkor $a \equiv 0^2 \pmod{p}$. Ha $p \nmid a$, akkor $p \perp a$, és így az 5.17. Tétel szerint a akkor és csak akkor négyzetes maradék modulo p, ha $\operatorname{ind}_g a$-nak osztója $\operatorname{Inko}(2, \varphi(p)) = \operatorname{Inko}(2, p-1) = 2$. □

5.20. Definíció.

Tetszőleges p páratlan prímszám és p-vel nem osztható a egész szám esetén értelmezzük az $\left(\frac{a}{p}\right)$ *Legendre-szimbólumot* a következőképpen:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ négyzetes maradék } \bmod p; \\ -1, & \text{ha } a \text{ négyzetes nemmaradék } \bmod p. \end{cases}$$

Euler-kritérium

5.21. Tétel (Euler-kritérium).

Ha p páratlan prímszám és $p \nmid a$, akkor

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Bizonyítás.

Legyen g primitív gyök modulo p, és számítsuk ki az $x := g^{\frac{p-1}{2}}$ hatványt modulo p. Tudjuk, hogy $x^2 \equiv g^{p-1} \equiv 1 \pmod{p}$ (miért?), így $p \mid x^2 - 1 = (x-1)(x+1)$.

Mivel p prím, $p \mid x-1$ vagy $p \mid x+1$. Az első esetben $x \equiv 1 \pmod{p}$, ami azt jelenti, hogy $o_p(g) \leq \frac{p-1}{2}$, de ez ellentmondás (miért?). Tehát csak a második eset lehetséges, azaz $x \equiv -1 \pmod{p}$.

Ennek alapján ki tudjuk számítani $a^{\frac{p-1}{2}}$ értékét modulo p:

$$a^{\frac{p-1}{2}} \equiv \left(g^{\operatorname{ind} a}\right)^{\frac{p-1}{2}} \equiv \left(g^{\frac{p-1}{2}}\right)^{\operatorname{ind} a} \equiv (-1)^{\operatorname{ind} a} \pmod{p}.$$

Az utóbbi hatvány aszerint lesz 1 vagy -1, hogy $\operatorname{ind} a$ páros-e vagy páratlan, vagyis, hogy a négyzetes maradék-e modulo p vagy sem (lásd az 5.19. Tételt). □

A Legendre-szimbólum alaptulajdonságai

5.22. Tétel.

Tetszőleges p páratlan prímszám és p-vel nem osztható a, b egész számok esetén teljesülnek az alábbiak:

(1) $a \equiv b \pmod{p} \implies (\frac{a}{p}) = (\frac{b}{p})$;

(2) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.

Bizonyítás.

Az első állítás triviális, mert $a \equiv b$ esetén az $x^2 \equiv a$ és $x^2 \equiv b$ kongruenciák ekvivalensek. A második állítás bizonyításának kulcsa az Euler-kritérium:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod{p}.$$

Mindkét oldalon 1 vagy -1 áll, és $1 \not\equiv -1 \pmod{p}$ (miért?), ezért a két oldal egyenlő egymással. □

Kvadratikus reciprocitás

5.23. Tétel.

Tetszőleges p páratlan prímszám esetén

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod 4; \\ -1, & \text{ha } p \equiv 3 \pmod 4. \end{cases}$$

5.24. Tétel (négyzetes reciprocitási tétel).

Tetszőleges p, q különböző páratlan prímszámok esetén

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}.$$

5.25. Tétel.

Tetszőleges p páratlan prímszámra

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{ha } p \equiv 1, 7 \pmod 8; \\ -1, & \text{ha } p \equiv 3, 5 \pmod 8. \end{cases}$$

Eljárás a Legendre-szimbólum kiszámítására

$$\left(\frac{7}{31}\right) \overset{\text{QR}}{=} -\left(\frac{31}{7}\right) \overset{\text{mod}}{=} -\left(\frac{3}{7}\right) \overset{\text{QR}}{=} \left(\frac{7}{3}\right) \overset{\text{mod}}{=} \left(\frac{1}{3}\right) = 1$$

$$\left(\frac{7}{31}\right) \overset{\text{QR}}{=} -\left(\frac{31}{7}\right) \overset{\text{mod}}{=} -\left(\frac{-4}{7}\right) \overset{\text{mult.}}{=} -\left(\frac{-1}{7}\right)\left(\frac{4}{7}\right) = -(-1)\cdot 1 = 1$$

$$\left(\frac{141}{181}\right) \overset{\text{mult.}}{=} \left(\frac{3}{181}\right)\left(\frac{47}{181}\right) \overset{\text{QR}}{=} \left(\frac{181}{3}\right)\left(\frac{181}{47}\right) \overset{\text{mod}}{=} \left(\frac{1}{3}\right)\left(\frac{40}{47}\right) \overset{\text{mult.}}{=} \left(\frac{2}{47}\right)^3\left(\frac{5}{47}\right)$$

$$= \left(\frac{5}{47}\right) \overset{\text{QR}}{=} \left(\frac{47}{5}\right) \overset{\text{mod}}{=} \left(\frac{2}{5}\right) = -1$$

modulo nevező redukáljuk (5.22/(1)) $\longrightarrow$ szétszedjük (5.22/(2))

$\uparrow$ $\downarrow$

fejreállítjuk (5.24) $\longleftarrow$ kiszámoljuk (5.23, 5.25)