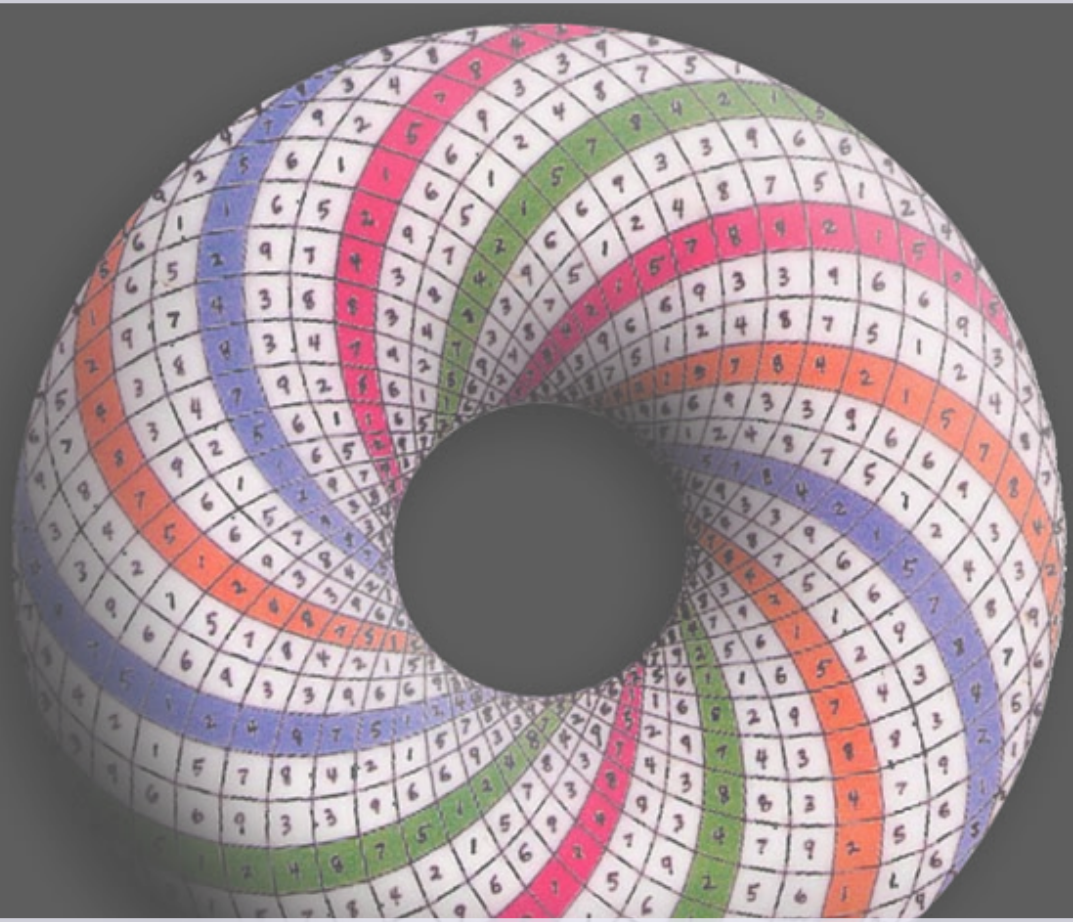
Kongruences un to lietojumi



Mārtiņš Kokainis

Latvijas Universitāte, NMS

Rīga, 2013

Saturs

1. Pamatjēdzieni
   - Ievads
   - Kongruences definīcija
   - Aritmētiskās darbības
2. Pēdējais cipars
3. Skaitļa pakāpes
4. Dalāmības pazīme ar 11
5. Modular art

Pamatjēdzieni

Dalāmība

1. definīcija

Saka, ka vesels skaitlis m dalās ar veselu skaitli n ($n \neq 0$) un pieraksta $m \vdots n$, ja eksistē tāds vesels skaitlis k, ka $m = n \cdot k$.

Piemēram,

- $9 \vdots 3$, jo $9 = 3 \cdot 3$.
- $142 \vdots 71$, jo $142 = 71 \cdot 2$.
- $142 \vdots (-71)$, jo $142 = (-71) \cdot (-2)$.
- $(-35) \vdots (-7)$, jo $-35 = (-7) \cdot 5$.

Dalīšana ar atlikumu

2. definīcija

Izdalīt veselu skaitli m ar **naturālu skaitli** n ar atlikumu nozīmē atrast tādus veselus skaitļus q un r, kuriem izpildās vienādība $m = q \cdot n + r$, turklāt $r = 0, 1, 2, \ldots, n - 1$.
Ja $r = 0$, tad sakām, ka m dalās ar n bez atlikuma (jeb, ka m dalās ar n).

- 29 dalot ar 5, iegūst dalījumu 5 un atlikumu 4, jo $29 = 5 \cdot 5 + 4$.
- -29 dalot ar 5, iegūst dalījumu -6 un atlikumu 1, jo $-29 = (-6) \cdot 5 + 1$.
- -24 dalot ar 3, iegūst dalījumu -8 un atlikumu 0, jo $-24 = (-8) \cdot 3 + 0$.

Skaitļu sadalījums klasēs

- Veselo skaitļu iedalījums pāra un nepāra skaitļos:
  - $\ldots, -4, -2, 0, 2, 4, \ldots$ – skaitļi, kas dalās ar 2 (pāra skaitļi);
  - $\ldots, -3, -1, 1, 3, 5, \ldots$ – skaitļi, kas nedalās ar 2 (nepāra skaitļi).
- Šī iedalījuma vispārinājums?
  - $\ldots, -3, 0, 3, 6, \ldots$ – skaitļi, kas dalās ar 3;
  - $\ldots, -2, -1, 1, 2, 4, 5, \ldots$ – skaitļi, kas nedalās ar 3.

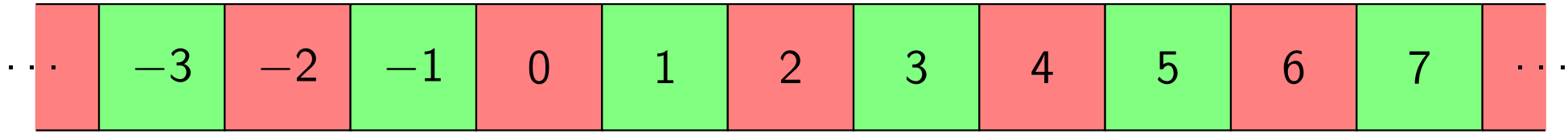
Skaitļu sadalījums klasēs

- Skaitļu sadalījums atkarībā no tā, kādus atlikumus tie dod, dalot ar 3:
  - $\ldots, -6, -3, 0, 3, \ldots$ – skaitļi, kuri, dalot ar 3, dod atlikumu 0;
  - $\ldots, -5, -2, 1, 4, \ldots$ – skaitļi, kuri, dalot ar 3, dod atlikumu 1;
  - $\ldots, -4, -1, 2, 5, \ldots$ – skaitļi, kuri, dalot ar 3, dod atlikumu 2.

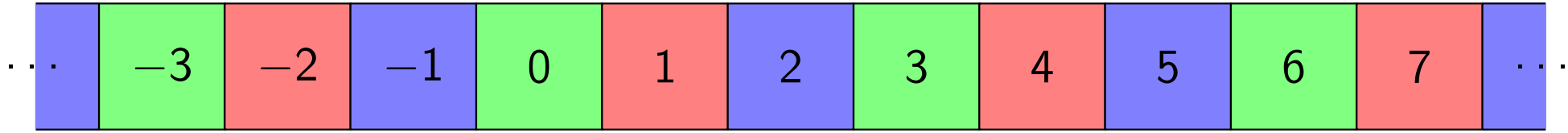
$\cdots$	-3	-2	-1	0	1	2	3	4	5	6	7	$\cdots$

Skaitļu krāsošana

- Skaitļu krāsošana atkarībā no atlikuma, dalot skaitļus ar 2:



- Skaitļu krāsošana atkarībā no atlikuma, dalot skaitļus ar 3:



Kongruences jēdziens

- Kongruences jēdziens – formalizē aplūkoto skaitļu "krāsošanu".

3. definīcija

Doti veseli skaitļi a un b un naturāls skaitlis $n \geq 2$. Saka, ka skaitļi a un b ir kongruenti pēc moduļa n un pieraksta $a \equiv b \pmod{n}$, ja a un b, dalot tos ar n, dod vienādus atlikumus.

- $3 \equiv 5 \pmod{2}$, jo 5 un 3 abi dod atlikumu 1, dalot ar 2;
- $4 \equiv -2 \pmod{3}$, jo 4 un -2 abi dod atlikumu 1, dalot ar 3;
- $-4 \equiv 87 \pmod{7}$, jo -4 un 87 abi dod atlikumu 3, dalot ar 7.

1. uzdevums

Vai sekojošās kongruences ir pareizas?

- $3 \equiv 7 \pmod 4$?

  Jā, jo gan 3, gan 7 dod atlikumu 3, dalot ar 4;

- $3 \equiv 7 \pmod 3$?

  Nē, jo 3 dod atlikumu 0, dalot ar 3, bet 7 dod atlikumu 1, dalot ar 3;

- $17 \equiv 73 \pmod{14}$?

  Jā, jo gan 17, gan 73 dod atlikumu 3, dalot ar 14;

- $71 \equiv 8 \pmod 9$?

  Jā, jo gan 71, gan 8 dod atlikumu 8, dalot ar 9.

Kongruences jēdziens

Vai ir pareizas sekojošās kongruences:

- $1 \equiv 4 \pmod 3$;
- $1 \equiv 7 \pmod 3$;
- $1 \equiv 10 \pmod 3$;
- $1 \equiv 13 \pmod 3$;
- $4 \equiv 7 \pmod 3$;
- $4 \equiv 10 \pmod 3$;
- $10 \equiv 16 \pmod 3$?

Kongruences jēdziens

Vai ir pareizas sekojošās kongruences:

- $2 \equiv 5 \pmod 3$;
- $2 \equiv 8 \pmod 3$;
- $2 \equiv 14 \pmod 3$;
- $5 \equiv 11 \pmod 3$;
- $11 \equiv 17 \pmod 3$?

Ko varam pateikt, ja divu skaitļu starpība dalās ar 3?

Ko varam pateikt, ja divu skaitļu starpība dalās ar 5?

Ko varam pateikt, ja divu skaitļu starpība dalās ar n?

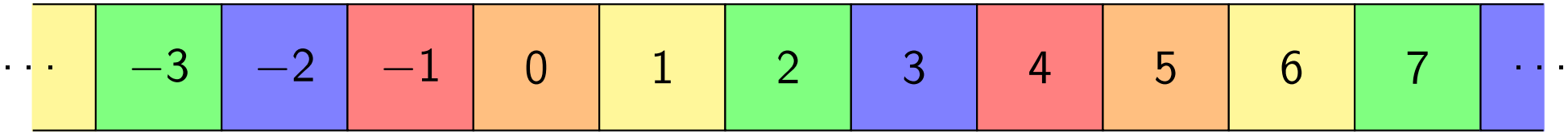
Kongruences jēdziens

1. teorēma

$a \equiv b \pmod{n}$ tad un tikai tad, ja starpība $a - b$ dalās ar n.

- $3 \equiv 5 \pmod{2}$, jo $5 - 3 = 2$ dalās ar 2;
- $4 \equiv -2 \pmod{3}$, jo $4 - (-2) = 6 = 3 \cdot 2$ dalās ar 3;
- $-6 \equiv 85 \pmod{7}$, jo $-6 - 85 = -91 = 7 \cdot (-13)$ dalās ar 7;
- $17 \equiv 73 \pmod{14}$, jo $17 - 73 = -56 = 14 \cdot (-4)$ dalās ar 14;
- $71 \equiv 8 \pmod{9}$, jo $71 - 8 = 63 = 9 \cdot 7$ dalās ar 9.

Kongruences jēdziens



- Skaitļi, kas kongruenti ar 0 pēc moduļa 5 – oranži;
- Skaitļi, kas kongruenti ar 1 pēc moduļa 5 – dzelteni;
- Skaitļi, kas kongruenti ar 2 pēc moduļa 5 – zaļi;
- Skaitļi, kas kongruenti ar 3 pēc moduļa 5 – zili;
- Skaitļi, kas kongruenti ar 4 pēc moduļa 5 – sarkani.

Kongruenču īpašības

- Visiem veseliem skaitļiem a izpildās kongruence $a \equiv a \pmod{n}$ (refleksivitāte);
- Ja $a \equiv b \pmod{n}$, tad $b \equiv a \pmod{n}$ (simetrija);
- Ja $a \equiv b \pmod{n}$ un $b \equiv c \pmod{n}$, tad $a \equiv c \pmod{n}$ (transitivitāte).

- Ja $a \equiv b \pmod{n}$ un $c \equiv d \pmod{n}$, tad
  1. $a + c \equiv b + d \pmod{n}$;
  2. $a - c \equiv b - d \pmod{n}$;
  3. $a \cdot c \equiv b \cdot d \pmod{n}$;
  4. $a^m \equiv b^m \pmod{n}$, visiem naturāliem skaitļiem m.

1. piemērs

Aprēķināt atlikumu, kāds rodas, skaitli $A = 113^2 + 21^7 - 43 \cdot 15$ dalot ar 11!

Jāaprēķina, ar ko kongruents A pēc moduļa 11:

$$113^2 + 21^7 - 43 \cdot 15 \equiv ? \pmod{11}$$

Veiksim aprēķinus pēc moduļa 11, izmantojot kongruenču īpašības:

$$113 = 110 + 3 = 11 \cdot 10 + 3 \equiv 3 \pmod{11};$$
$$21 = 22 - 1 = 11 \cdot 2 - 1 \equiv -1 \pmod{11};$$
$$43 = 44 - 1 = 11 \cdot 4 - 1 \equiv -1 \pmod{11};$$
$$15 \equiv 11 + 4 \equiv 4 \pmod{11}.$$

1. piemērs

Tātad $113^2 + 21^7 - 43 \cdot 15 \equiv 3^2 + (-1)^7 - (-1) \cdot 4 \pmod{11}$.

$$A \equiv 9 - 1 + 4 \equiv 12 \equiv 1 \pmod{11}.$$

Līdz ar to secinām, ka skaitli A, dalot ar 11, atlikums ir 1.

2. uzdevums

Aprēķināt atlikumu, skaitli A dalot ar n!

- $A = 13^3 - 49 \cdot 7 + 220^{220} \cdot 24, \quad n = 12;$
- $A = 23^3 - 57 \cdot 12^2 - 81 \cdot 44, \quad n = 7;$
- $A = 15^2 - 321 \cdot 38 - 16^3 \cdot 5, \quad n = 19.$

2. uzdevums

Aplūkojam atbilstošās kongruences:

- $13^3 - 49 \cdot 7 + 220^{220} \cdot 12 \pmod{12}$;
- $23^3 - 57 \cdot 12^2 - 81 \cdot 44 \pmod{7}$;
- $15^2 - 321 \cdot 38 - 16^3 \cdot 5 \pmod{19}$.

2. uzdevums

$$13^3 - 49 \cdot 7 + 220^{220} \cdot 12 \equiv$$

$$\equiv 1^3 - 1 \cdot 7 + 220^{220} \cdot 0 \equiv$$

$$\equiv 1 - 7 \equiv -6 \equiv 6 \pmod{12};$$

2. uzdevums

$$23^3 - 57 \cdot 12^2 - 81 \cdot 44 \equiv$$

$$\equiv 2^3 - 1 \cdot (-2)^2 - 4 \cdot 2 \equiv$$

$$\equiv 8 - 1 \cdot 4 - 8 \equiv -4 \equiv 3 \pmod 7;$$

2. uzdevums

$$15^2 - 321 \cdot 38 - 16^3 \cdot 5 \equiv$$

$$\equiv (-4)^2 - 321 \cdot 0 - (-3)^3 \cdot 5 \equiv$$

$$\equiv 16 - (-27) \cdot 5 \equiv$$

$$\equiv -3 + 27 \cdot 5 \equiv$$

$$\equiv -3 + 8 \cdot 5 \equiv 37 \equiv -1 \equiv 18 \pmod{19}.$$

2. piemērs

Pierādīt, ka visiem naturāliem n skaitlis $2 \cdot 5^{2n} + 14^n - 3^{n+1}$ dalās ar 11!

- Vispirms izmantojam pakāpju īpašības: $5^{2n} = 25^n$, $3^{n+1} = 3 \cdot 3^n$.
- Tātad jāpierāda, ka $2 \cdot 25^n + 14^n - 3 \cdot 3^n$ dalās ar 11.

- Jāpierāda, ka $2 \cdot 25^n + 14^n - 3 \cdot 3^n \equiv 0 \pmod{11}$.
- Ievērojam, ka $25 = 22 + 3 \equiv 3 \pmod{11}$, $14 \equiv 3 \pmod{11}$.

- Iegūstam, ka

$$2 \cdot 25^n + 14^n - 3 \cdot 3^n \equiv 2 \cdot 3^n + 3^n - 3 \cdot 3^n \equiv (2 + 1 - 3) \cdot 3^n \equiv 0 \pmod{11}.$$

Pēdējais cipars

Skaitļa pēdējais cipars

- Naturāla skaitļa pēdējais cipars – atlikums, to dalot ar 10.
- Naturāls skaitlis kongruents ar savu pēdējo ciparu pēc moduļa 10.

$$47 \equiv 7 \pmod{10};$$
$$123659 \equiv 9 \pmod{10};$$
$$1231^{78} \equiv 1^{78} \equiv 1 \pmod{10}.$$

- **NB!** Negatīviem skaitļiem šī kongruence nav spēkā:

$$-11 \not\equiv 1 \pmod{10}.$$

3. piemērs

Aprēķināt reizinājuma $13 \cdot 27 \cdot 49$ pēdējo ciparu!

Saskaņā ar kongruenču īpašībām

$$13 \cdot 27 \cdot 49 \equiv 3 \cdot 7 \cdot 9 \equiv 21 \cdot 9 \equiv 1 \cdot 9 \equiv 9 \pmod{10}.$$

Naturālu skaitļu summas (vai reizinājuma) pēdējais cipars ir atkarīgs tikai no saskaitāmo (reizinātāju) pēdējiem cipariem.

Skaitļa pakāpes

Skaitļa pakāpes

- Vai vesela skaitļa kvadrāts var dot atlikumu 2, dalot ar 3?
- Kādus atlikumus veselu skaitļu kvadrāti dod, dalot ar 3?

$n \pmod 3$	0	1	2
$n^2 \pmod 3$	$0^2 \equiv 0 \pmod 3$	$1^2 \equiv 1 \pmod 3$	$2^2 \equiv 4 \equiv 1 \pmod 3$

- Secinām: vesela skaitļa kvadrāts, dalot ar 3, var dot atlikumus 0 vai 1.
- $n^2 \in \{0; 1\} \pmod 3$.

4. piemērs

- Vai 2011201220132 ir vesela skaitļa kvadrāts?
- Izvilkt kvadrātsakni "uz papīra" - iespējams, bet darbietilpīgi.
- Taču $2011201220132 = 2011201220130 + 2$.
- Skaitlis 2011201220130 dalās ar 3, jo tā ciparu summa 15 dalās ar 3; tātad dotais skaitlis kongruents ar 2 pēc moduļa 3.
- Secinām: dotais skaitlis nav vesela skaitļa kvadrāts.

3. uzdevums

Vai var atrast tādu vesela skaitļa kvadrātu, kurš dod atlikumu 3, dalot ar 4?

3. uzdevums

- Atbilde: nē, nevar atrast.

$n \pmod 4$	0	1	2	3
$n^2 \pmod 4$	0	1	0	1

- Secinām: $n^2 \in \{0; 1\} \pmod 4$.

5. piemērs

Dots, ka a, b – naturāli skaitļi un $a^2 + b^2$ dalās ar 3. Pierādīt, ka $a^2 + b^2$ dalās ar 9!

- $a^2 \equiv 0 \pmod 3$ vai $a^2 \equiv 1 \pmod 3$;
- $b^2 \equiv 0 \pmod 3$ vai $b^2 \equiv 1 \pmod 3$;
- Atliksim iespējamās $a^2 + b^2$ vērtības (pēc moduļa 3) tabulā.

$b^2 \pmod 3$ \ $a^2 \pmod 3$	0	1
0	$0 + 0 \equiv 0 \pmod 3$	$1 + 0 \equiv 1 \pmod 3$
1	$0 + 1 \equiv 1 \pmod 3$	$1 + 1 \equiv 2 \pmod 3$

$a^2 + b^2$ dalās ar 3 tikai tad, ja a un b katrs dalās ar 3.
Taču tad gan a^2, gan b^2 dalās ar 9; tātad arī to summa dalās ar 9.

5. piemērs

- Faktiski pierādīts: nevar atrast tādus veselus skaitļus a, b, n, ka izpildītos kāda no vienādībām

$$a^2 + b^2 = 9n + 3$$

vai

$$a^2 + b^2 = 9n + 6.$$

4. uzdevums

Pierādīt, ka nevar atrast tādus veselus skaitļus n, x, y, ka

$$12n + 7 = x^2 - 3y^2 \ !$$

4. uzdevums

- Atrodam, kādus atlikumus var dot vesela skaitļa kvadrāts, dalot ar 12:

$a \pmod{12}$	0	1	2	3	4	5	6	7	8	9	10	11
$a^2 \pmod{12}$	0	1	4	9	4	1	0	1	4	9	4	1
$3a^2 \pmod{12}$	0	3	0	3	0	3	0	3	0	3	0	3

4. uzdevums

- $x^2 \in \{0; 1; 4; 9\} \pmod{12}$;
- $3y^2 \in \{0; 3\} \pmod{12}$;
- Sastādām tabulu, pa rindiņām apskatot iespējamās x^2 vērtības pēc moduļa 12, pa kolonnām $3y^2$ vērtības pēc moduļa 12, bet tabulas šūnās atliekot $x^2 - 3y^2 \pmod{12}$:

$3y^2 \pmod{12}$ \ $x^2 \pmod{12}$	0	1	4	9
0	0	1	4	9
3	9	10	1	6

- Secinām: $x^2 - 3y^2 \in \{0; 1; 4; 6; 9; 10\} \pmod{12}$.
- Tātad $x^2 - 3y^2 \neq 12n + 7$.

Dalāmības pazīme ar 11

Dalāmība ar 11

- Mazliet mazāk nekā citas ir zināma dalāmības pazīme ar 11:

Naturāls skaitlis dalās ar 11 tad un tikai tad, ja tā ciparu summa, kas atrodas pāra pozīcijās, mīnus ciparu summa, kas atrodas nepāra pozīcijās, dalās ar 11.

- "Pāra" un "nepāra" pozīcijas sāk skaitīt *no labās puses uz kreiso*, t.i., vienu skaits – nepāra pozīcija, desmitu skaits – pāra pozīcija, simtu skaits – nepāra pozīcija utt.

Vai skaitlis 43725 dalās ar 11?

- $S_1(43725) = 5 + 7 + 4 = 16$ – ciparu summa **nepāra** pozīcijās;
- $S_2(43725) = 2 + 3 = 5$ – ciparu summa **pāra** pozīcijās.
- Starpība $16 - 5 = 11$ dalās ar 11, tātad skaitlis 43725 dalās ar 11.

Dalāmība ar 11

Vai skaitlis 1331 dalās ar 11?

- $S_1(1331) = 1 + 3 = 4$ – ciparu summa **nepāra** pozīcijās;
- $S_2(1331) = 3 + 1 = 4$ – ciparu summa **pāra** pozīcijās.
- Starpība $4 - 4 = 0$ dalās ar 11, tātad skaitlis 1331 dalās ar 11.

Vai skaitlis 7621531 dalās ar 11?

- $S_1(7621531) = 1 + 5 + 2 + 7 = 15$ – ciparu summa **nepāra** pozīcijās;
- $S_2(7621531) = 3 + 1 + 6 = 10$ – ciparu summa **pāra** pozīcijās.
- Starpība $15 - 10 = 5$ nedalās ar 11, tātad 7621531 nedalās ar 11.

Modular art

Modular art – dažādu rakstu veidošana

"Saskaitīšanas tabula" pēc moduļa 5: sastādām tabulu,

- pa rindiņām apskatot iespējamās x vērtības pēc moduļa 5,
- pa kolonnām – y vērtības pēc moduļa 5,
- bet tabulas šūnās atliekot $x + y \pmod 5$.

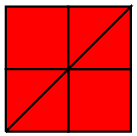
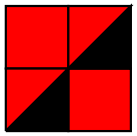
$y \pmod 5$ \ $x \pmod 5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Modular art – dažādu rakstu veidošana

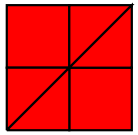
"Saskaitīšanas tabula" pēc moduļa 5:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Modular art – dažādu rakstu veidošana

- 0 aizstāj ar  ;
- 1 aizstāj ar  ;
- 2 aizstāj ar  ;
- 3 aizstāj ar  ;
- 4 aizstāj ar  .

Modular art – dažādu rakstu veidošana

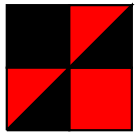
- Aizstājam 0 ar  :

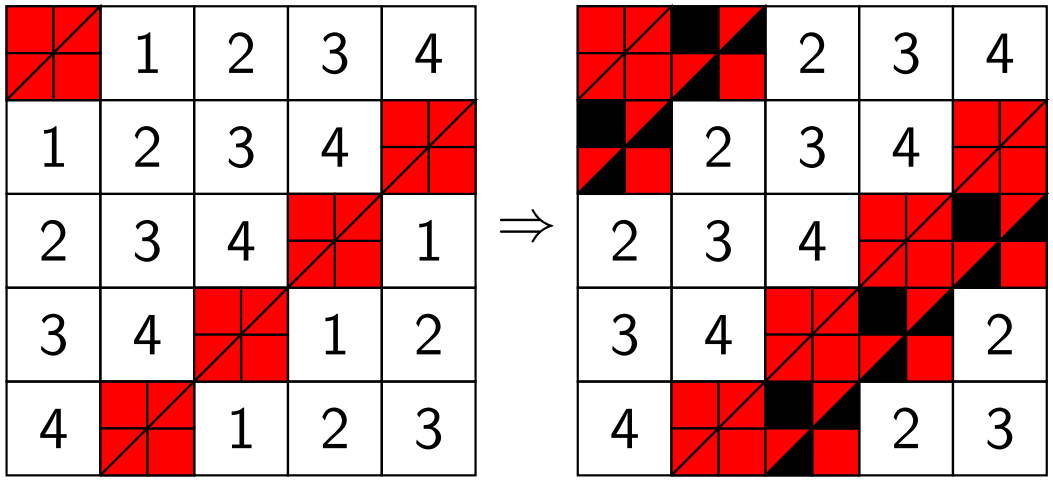
0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

$\Rightarrow$

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

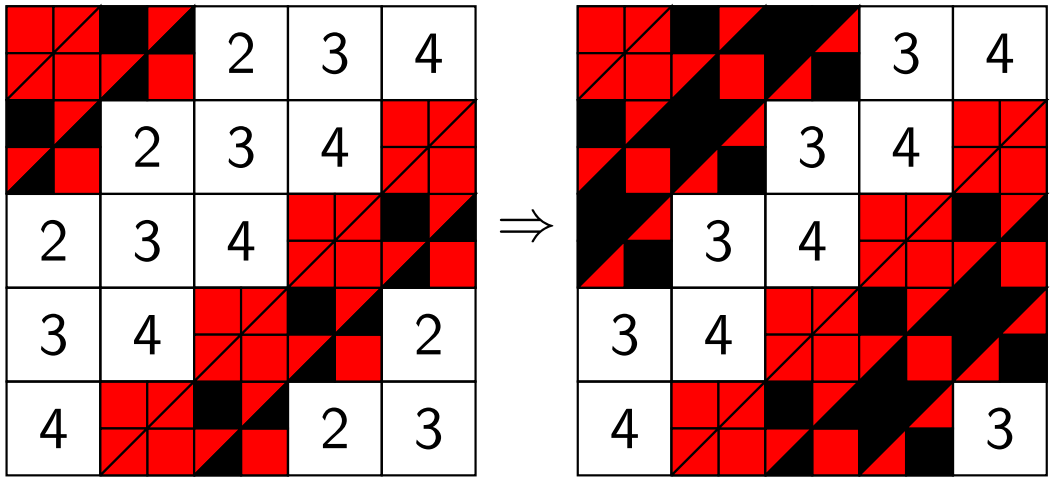
Modular art – dažādu rakstu veidošana

- Aizstājam 1 ar  :

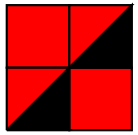


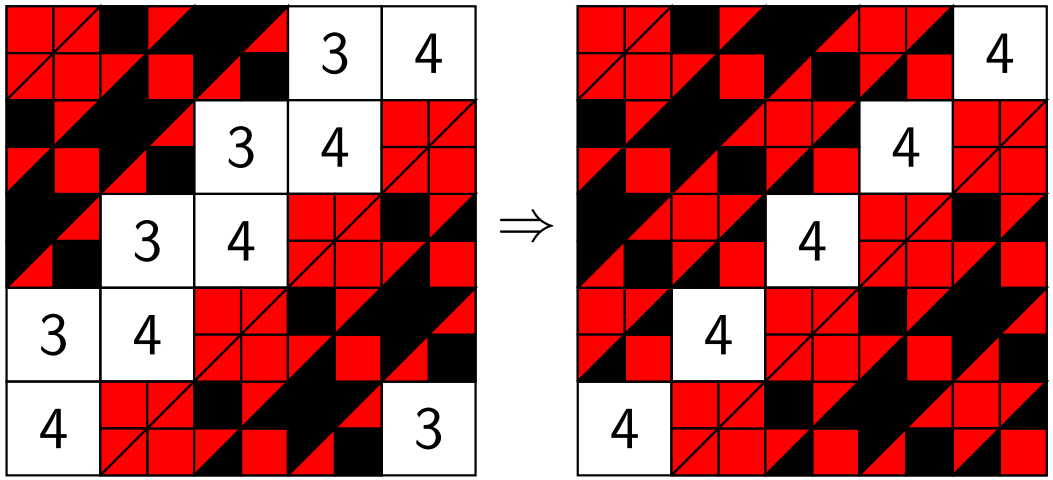
Modular art – dažādu rakstu veidošana

- Aizstājam 2 ar  :



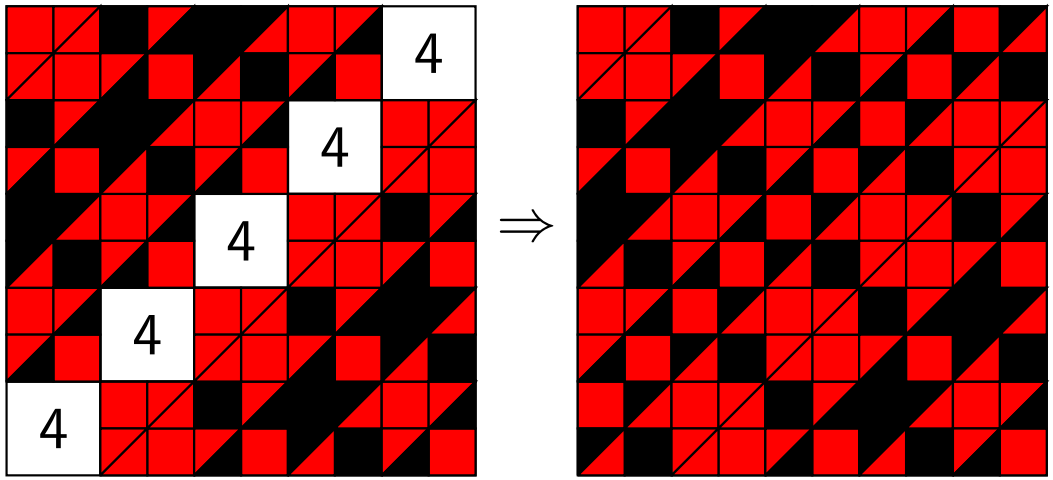
Modular art – dažādu rakstu veidošana

- Aizstājam 3 ar  :



Modular art – dažādu rakstu veidošana

- Aizstājam 4 ar  :

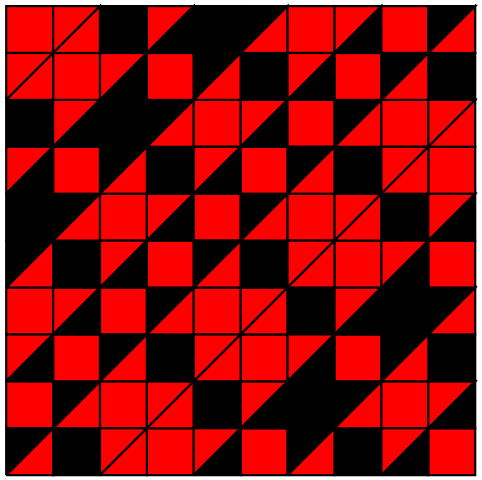


Modular art – dažādu rakstu veidošana

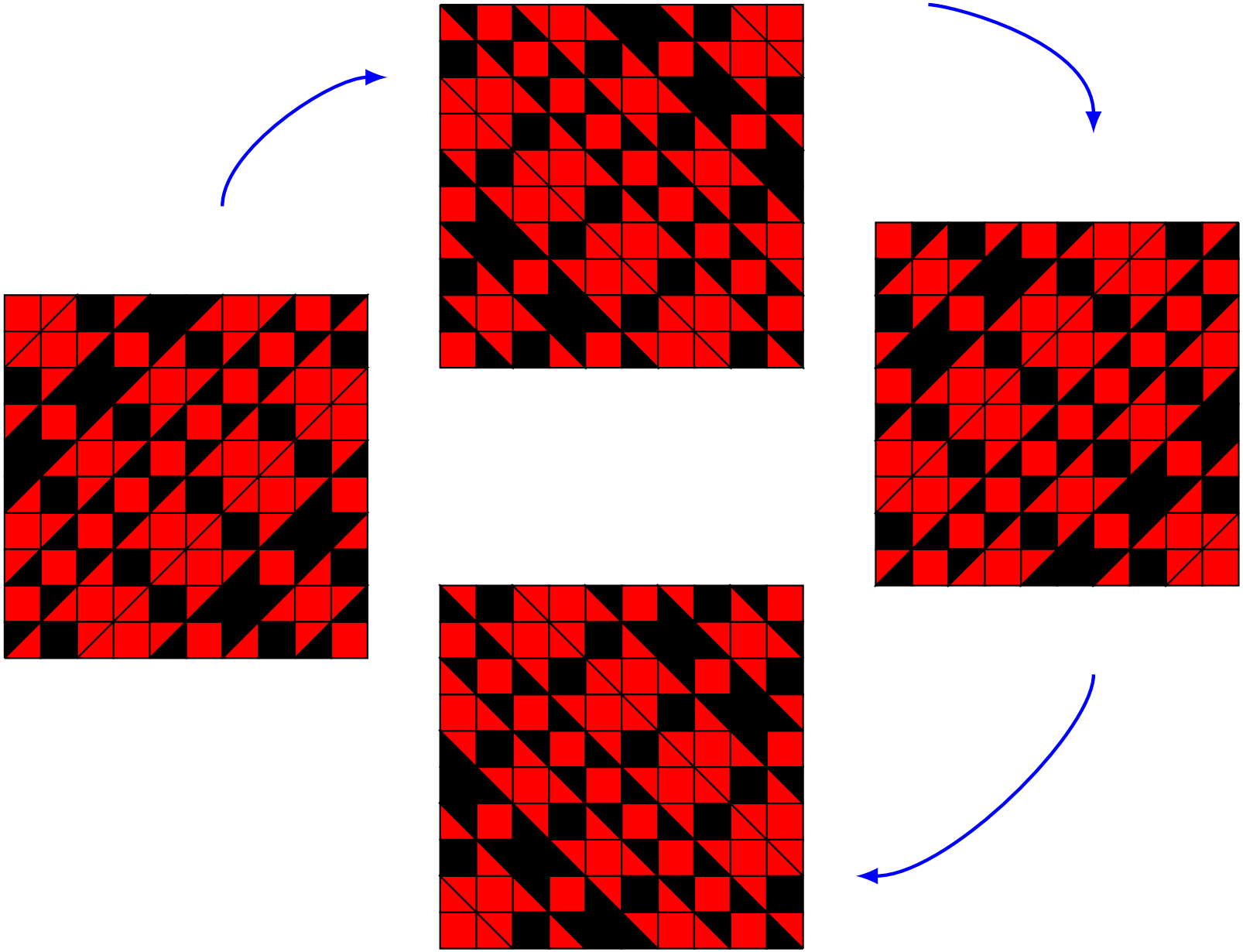
- "Saskaitīšanas tabula" tiek aizstāta ar grafisku rakstu:

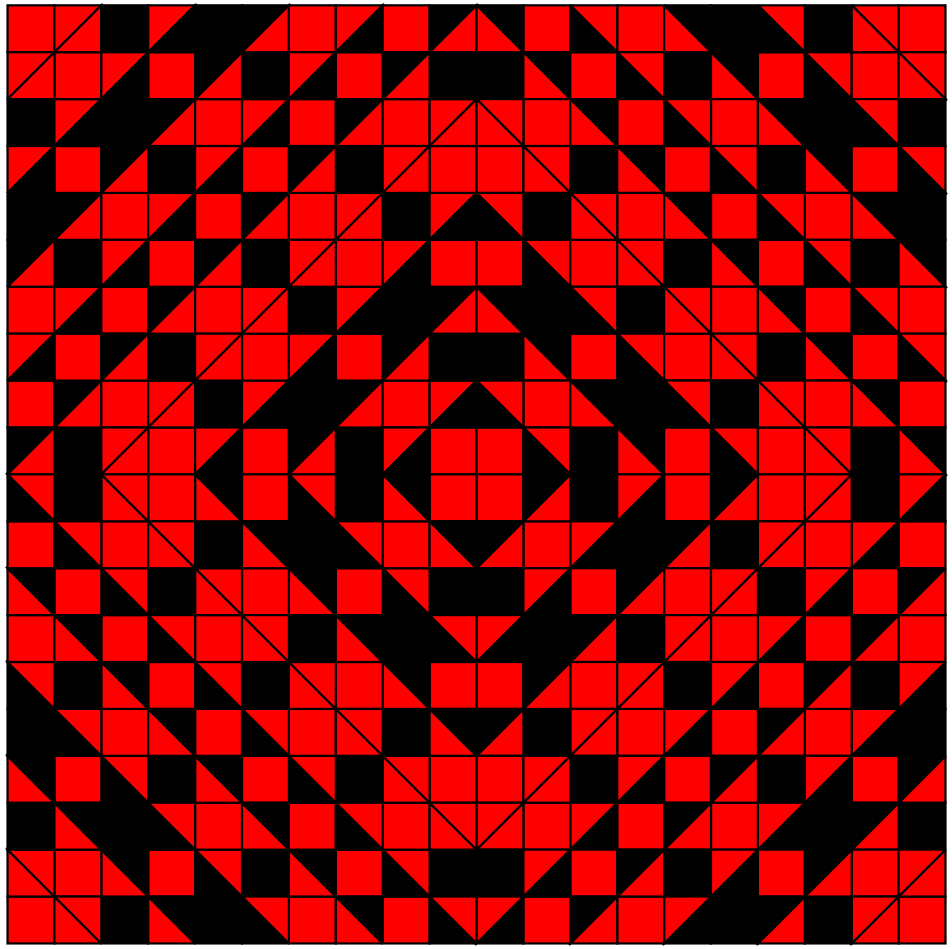
0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

$\Rightarrow$



- Rotējot iegūto rakstu, iegūst simetrisku attēlu.



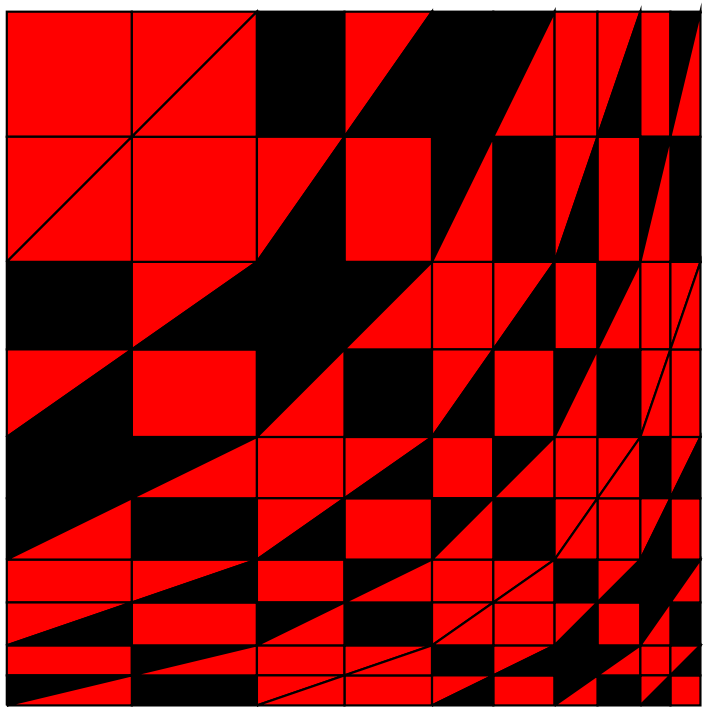


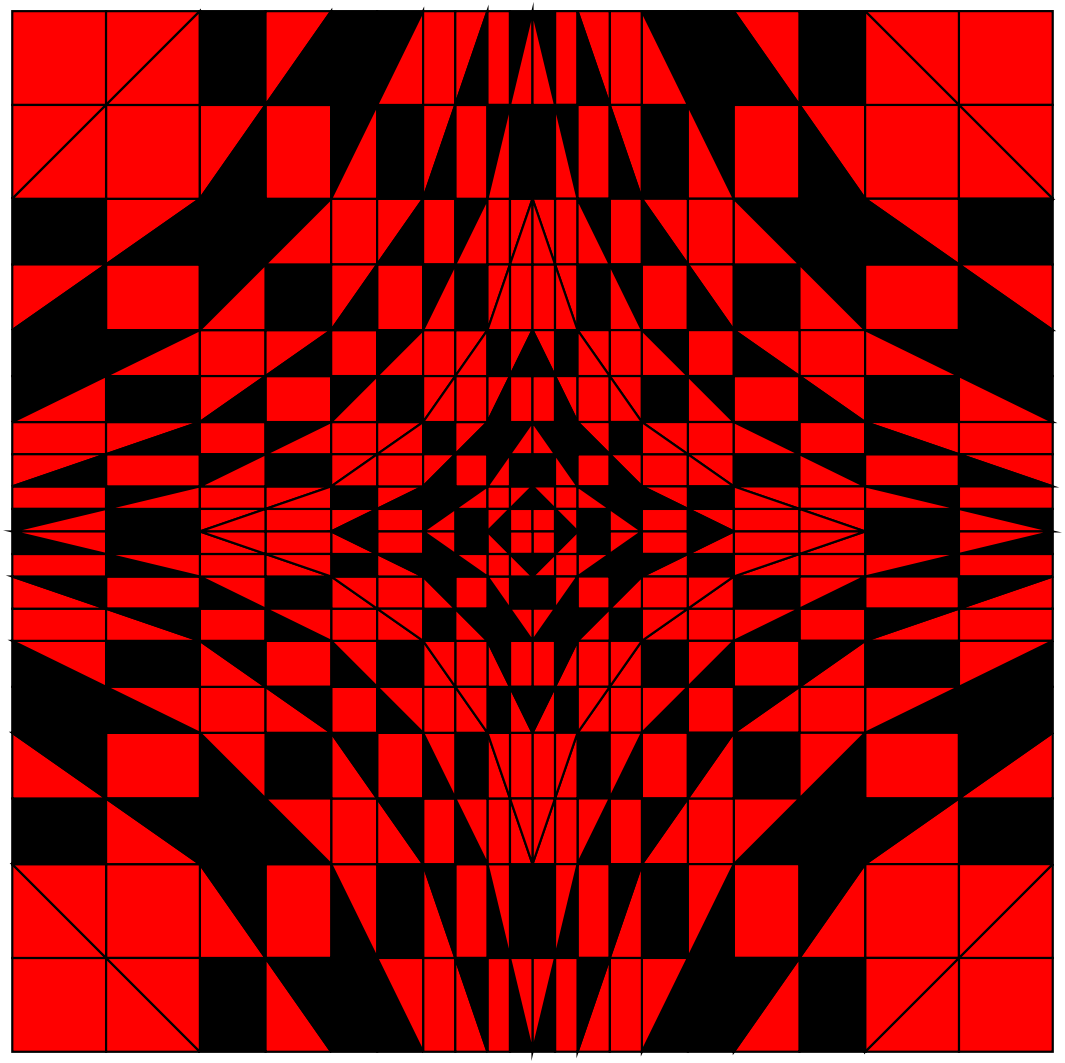
Modular art – dažādu rakstu veidošana

- Iespējams deformēt rūtiņu izmēru; piemērs, kad katra nākamā rūtiņa pa labi ir par 30% šaurāka nekā rūtiņa pa kreisi no tās un katras nākamās rūtiņas uz leju augstums ir par 30% mazāks nekā rūtiņai virs tās.

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

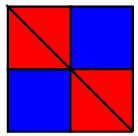
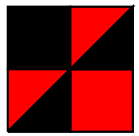
$\Rightarrow$

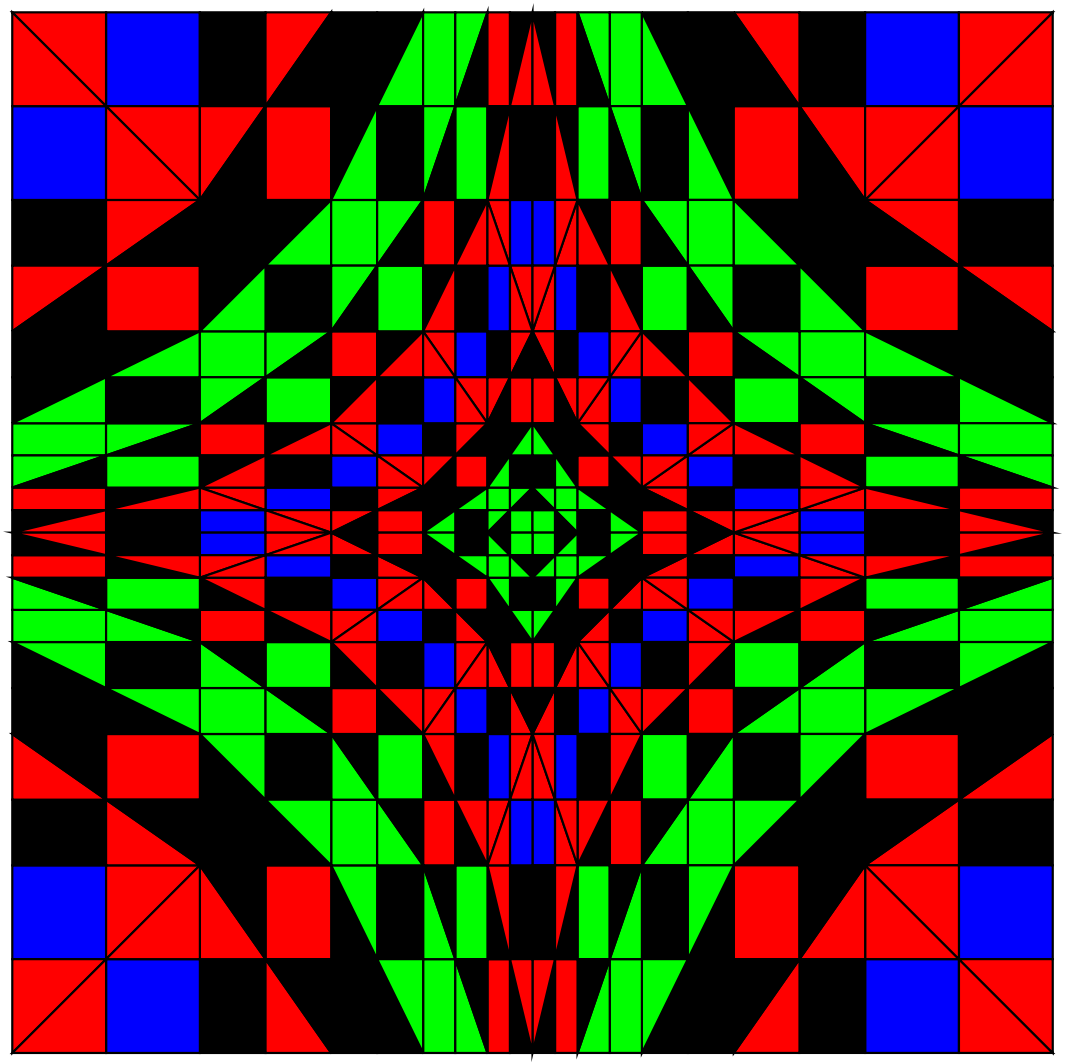




http://britton.disted.camosun.bc.ca/modart/jbmodart2.htm

Modular art – dažādu rakstu veidošana

- 0 aizstāj ar  ;
- 1 aizstāj ar  ;
- 2 aizstāj ar  ;
- 3 aizstāj ar  ;
- 4 aizstāj ar  .



Paldies par uzmanību!