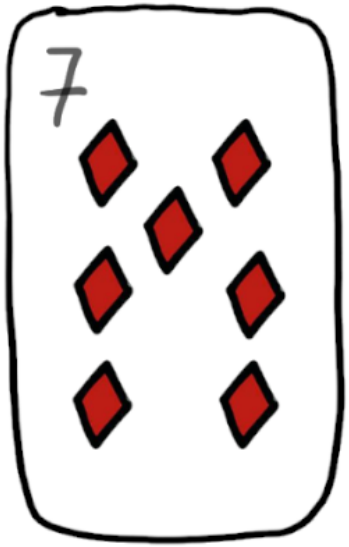
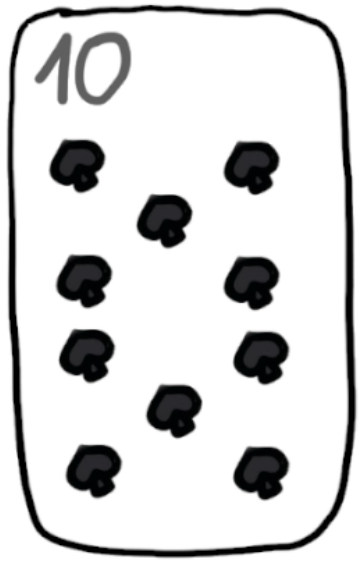
Gra w oczko, a rozwiązywanie równań wielomianowych



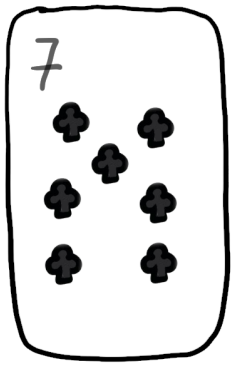
Jędrzej Garnek



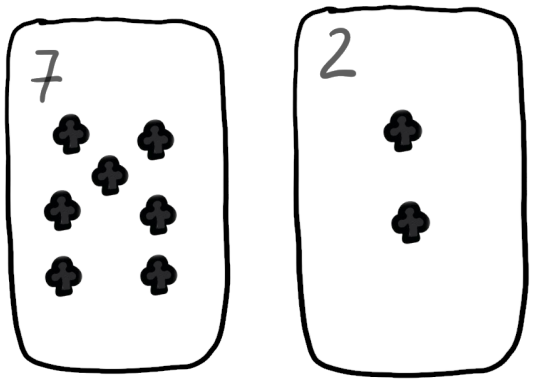
Zagrajmy w grę!

Nie-oczko:

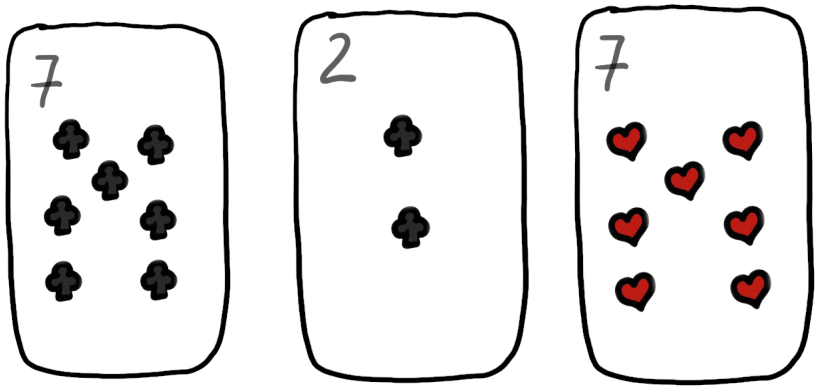
Nie-oczko:



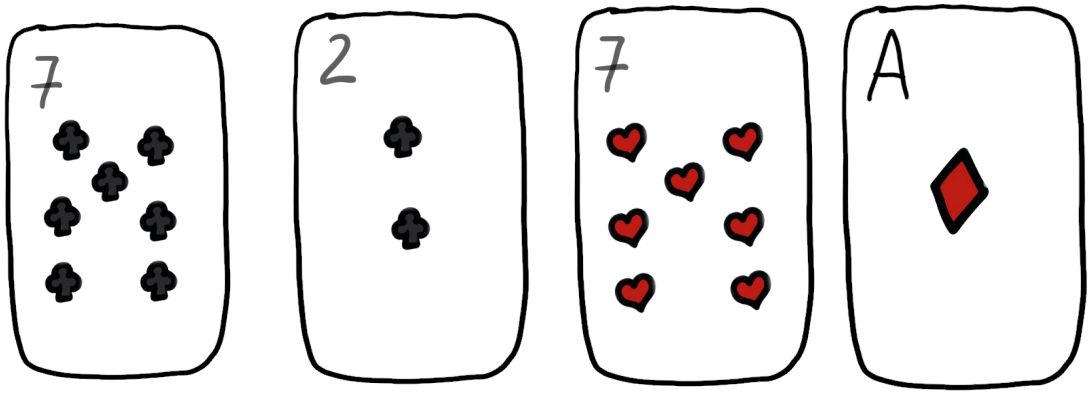
Nie-oczko:



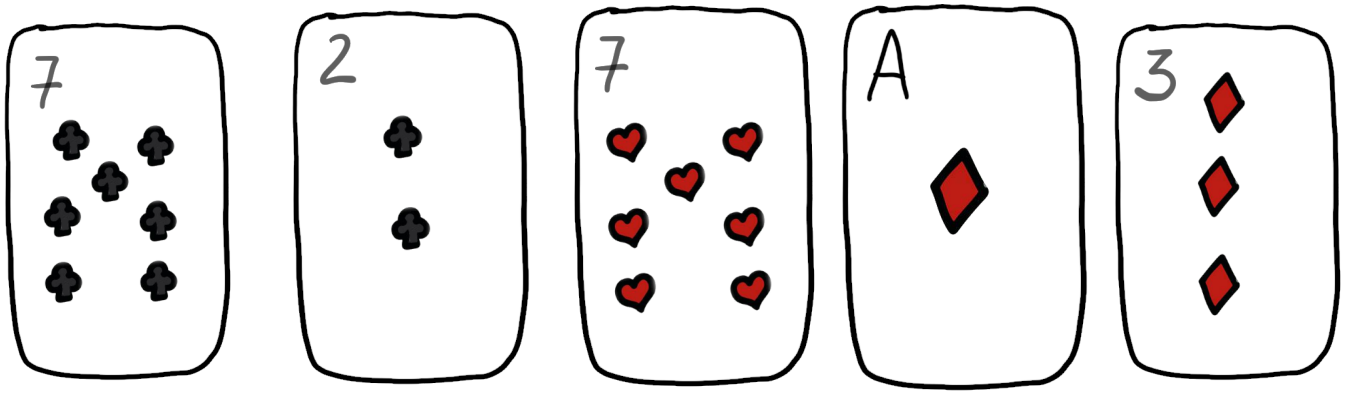
Nie-oczko:



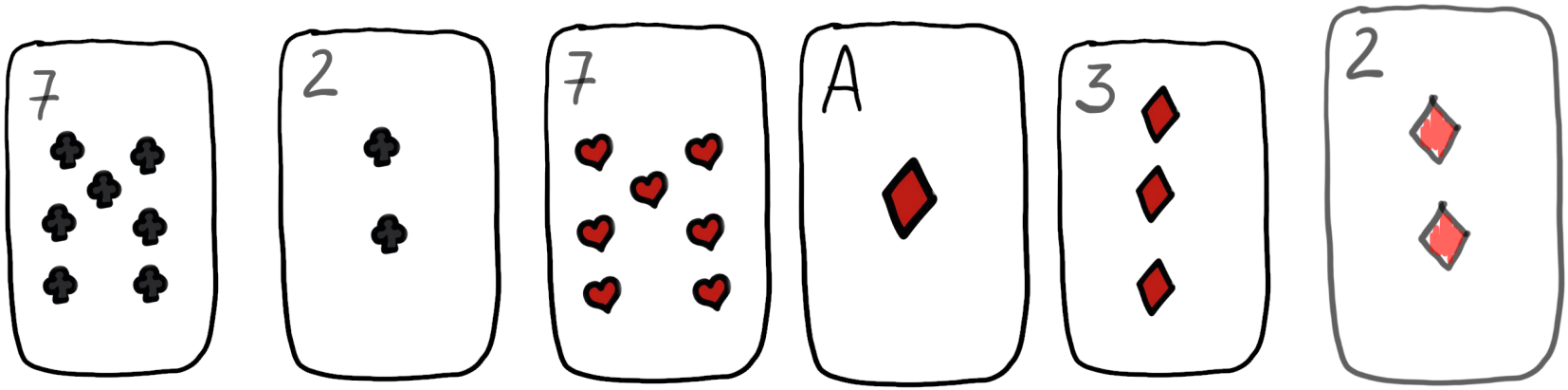
Nie-oczko:



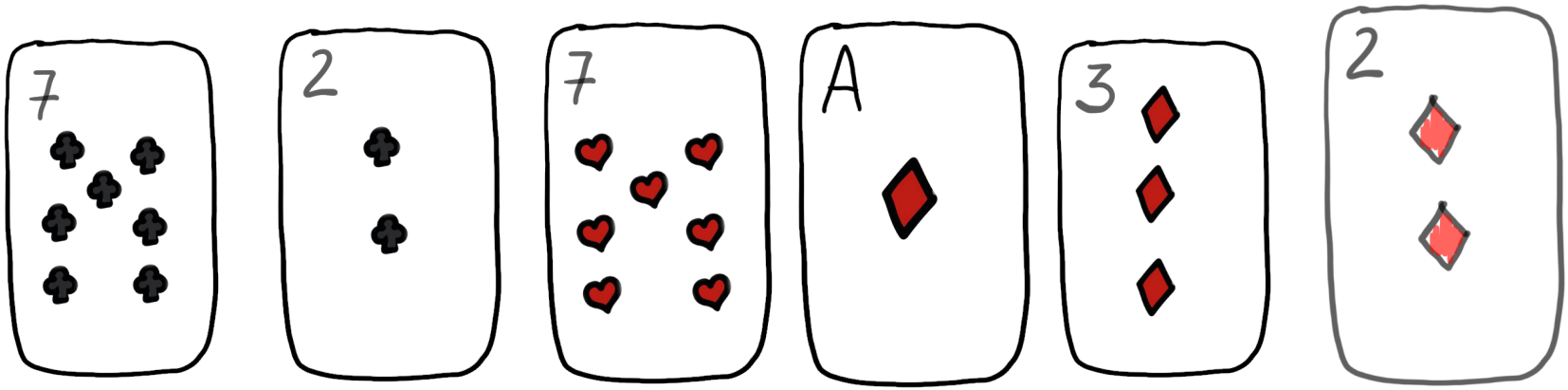
Nie-oczko:



Nie-oczko:



Nie-oczko:



Pytanie

Czy ta gra musi się skończyć?

Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. Wtedy istnieje niepusty zbiór $I \subset \{1, \ldots, n\}$ taki, że

$$n | \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,

Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,

Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.

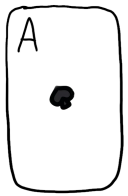
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



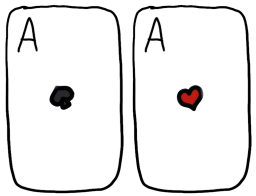
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



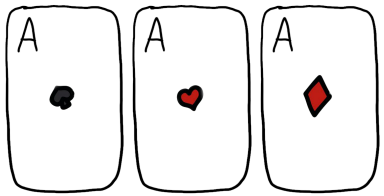
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



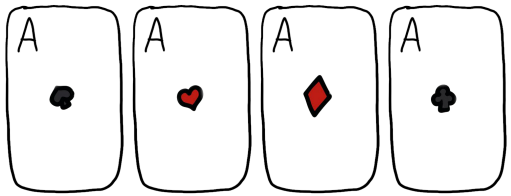
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



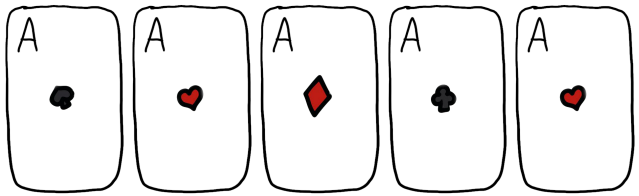
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



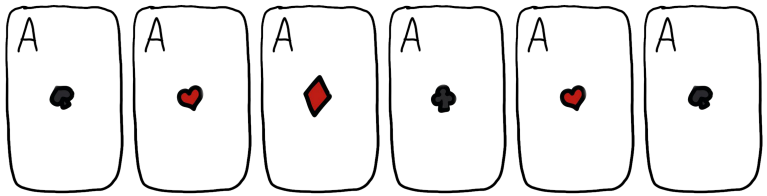
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



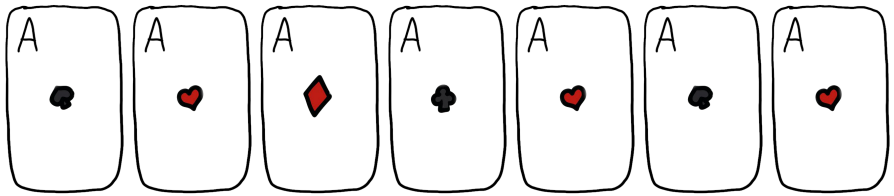
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



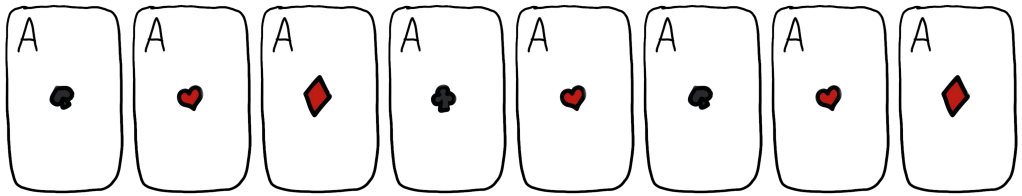
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



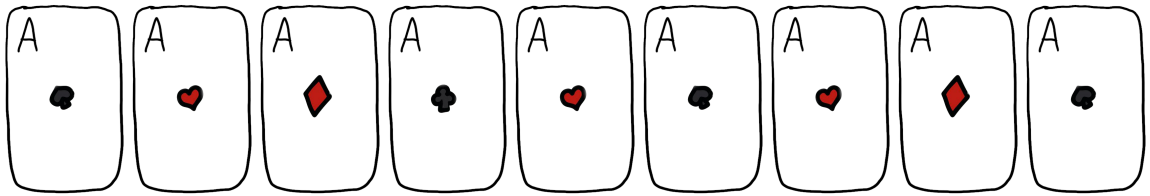
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



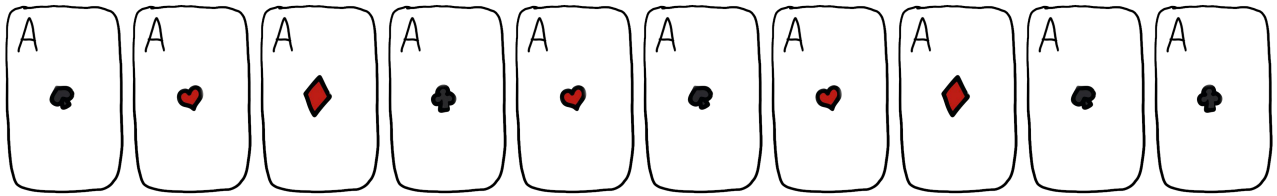
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



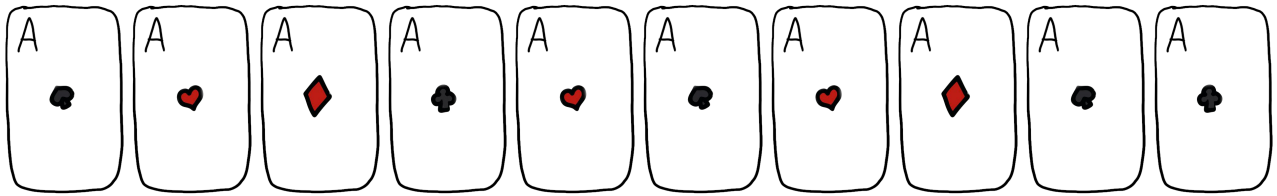
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



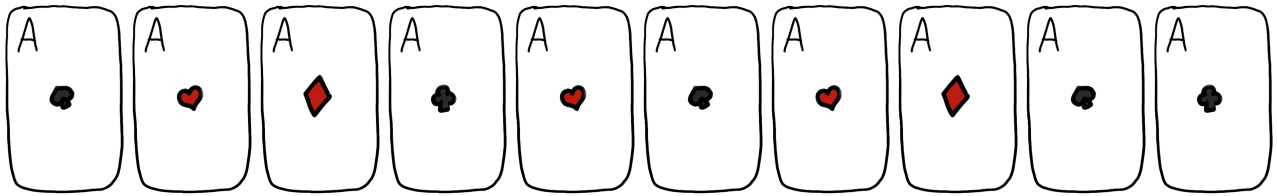
Fakt

Niech $a_1, a_2, \ldots \in \mathbb{Z}$. *Wtedy istnieje niepusty zbiór* $I \subset \{1, \ldots, n\}$ *taki, że*

$$n | \sum_{i \in I} a_i.$$

Dowód

- $S_k := a_1 + \ldots + a_k$,
- $(n+1)$-*kulek:* $S_0, \ldots, S_n$, $n+1$ *szufladek: reszty mod* n,
- $\exists_{k_1 < k_2} : S_{k_1} \equiv S_{k_2} \quad \Rightarrow \quad a_{k_1+1} + \ldots + a_{k_2} \equiv 0 \pmod{n}$.



Jeżeli $a_1 = a_2 = \ldots = 1$, to $n | \sum_{i \in I} a_i$ wtedy i tylko wtedy, gdy $n | \#I$!

Utrudnijmy naszą grę!

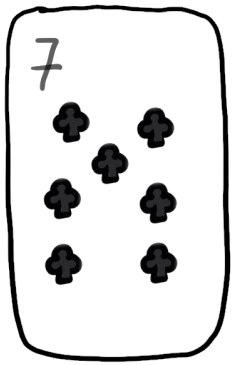
Pytanie

Od teraz będziemy wymagali, żeby wskazać ***6 kart*** *o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*

Utrudnijmy naszą grę!

Pytanie

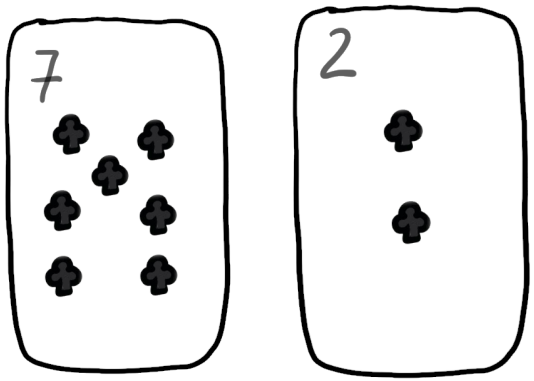
*Od teraz będziemy wymagali, żeby wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

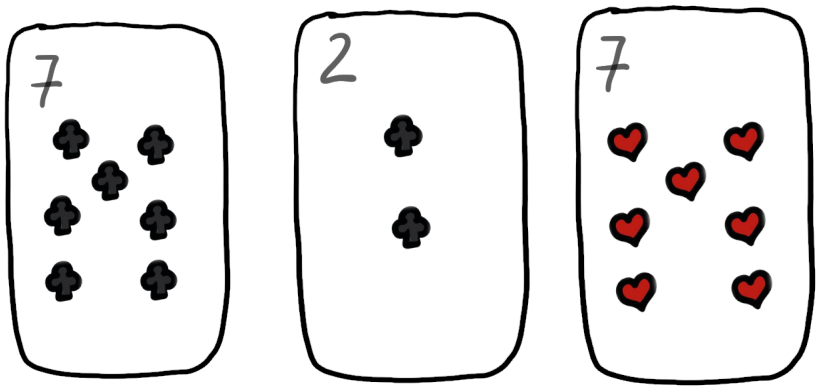
*Od teraz będziemy wymagali, żeby wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

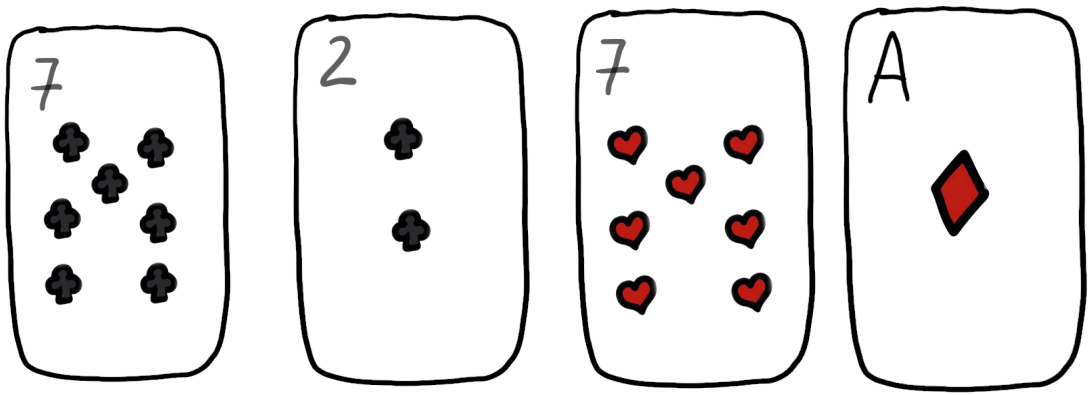
*Od teraz będziemy wymagali, żeby wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

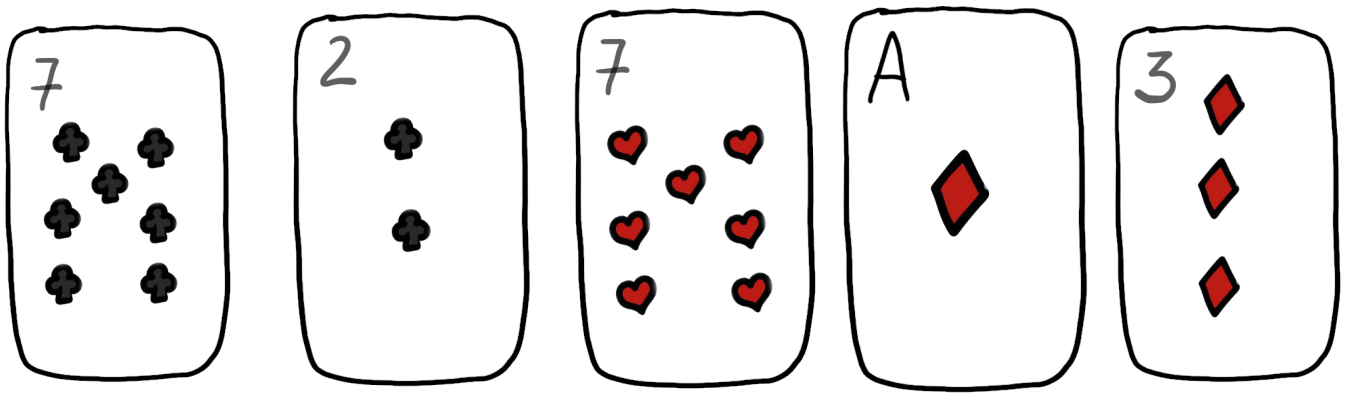
*Od teraz będziemy wymagali, żeby wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

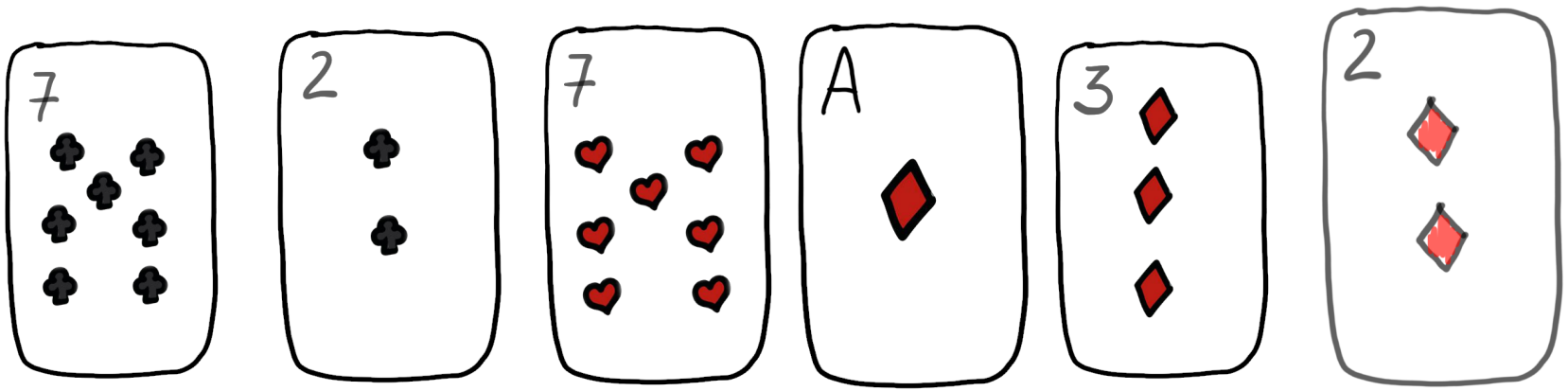
*Od teraz będziemy wymagali, żeby wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

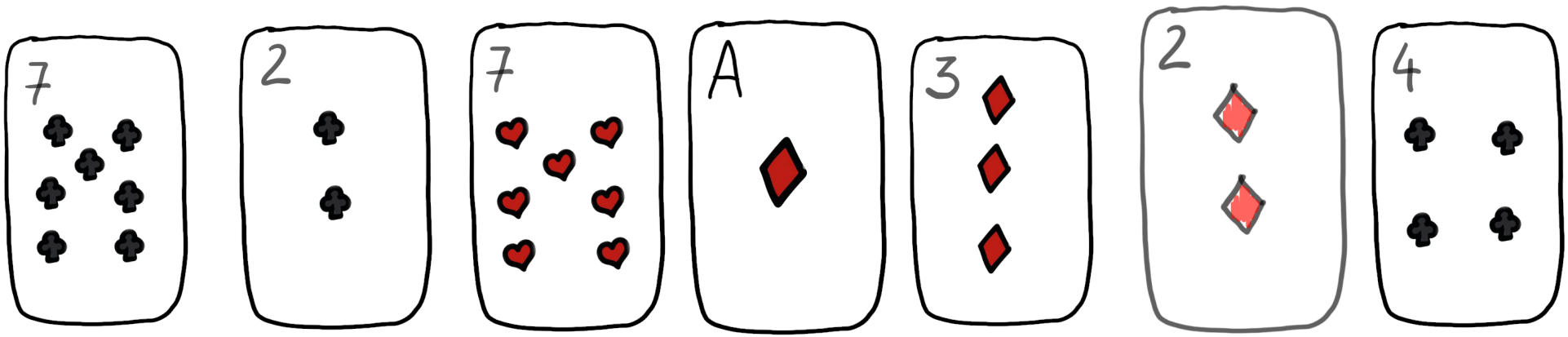
Od teraz będziemy wymagali, żeby wskazać ***6 kart*** *o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

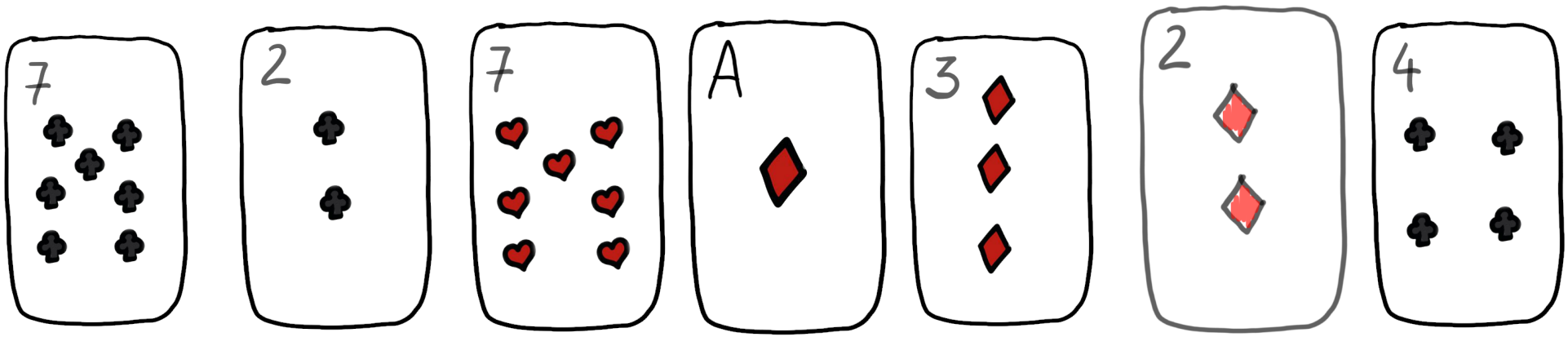
*Od teraz będziemy wymagali, żeby wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

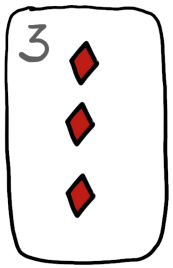
*Od teraz będziemy wymagali, żeby wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

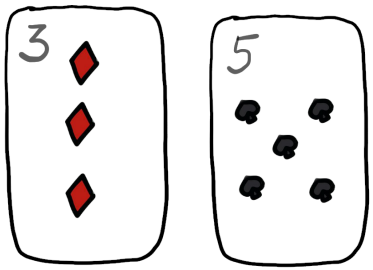
*Od teraz wymagamy, by wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

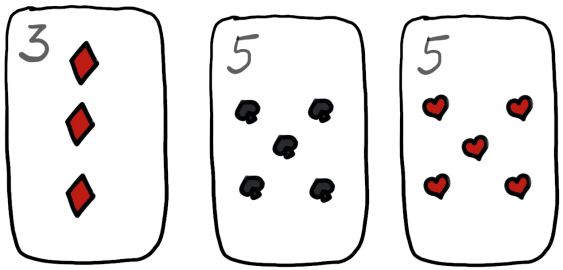
Od teraz wymagamy, by wskazać ***6 kart*** *o sumie podzielnej przez* 6. *Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

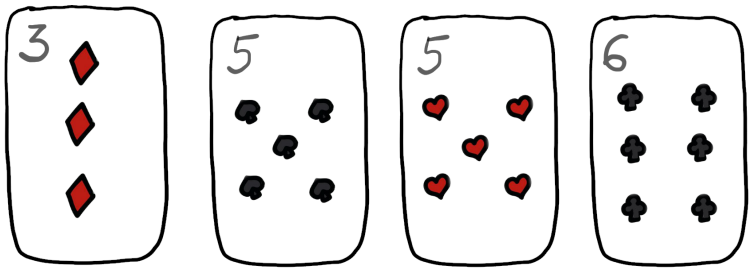
*Od teraz wymagamy, by wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

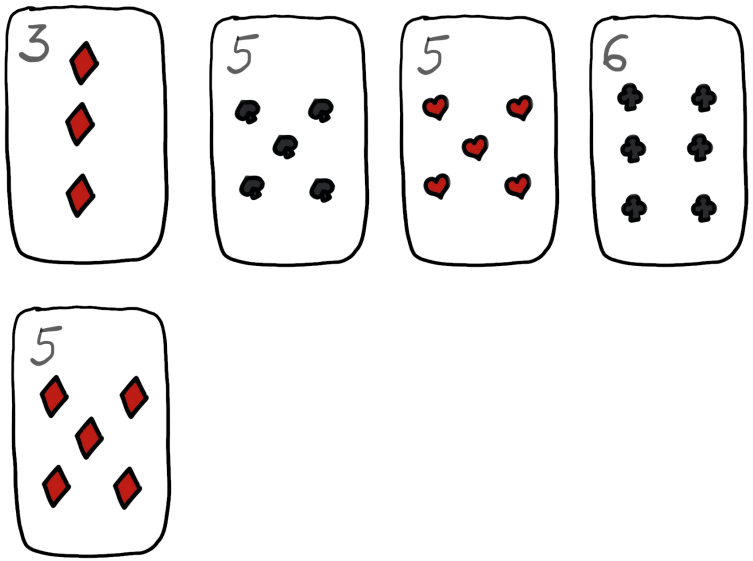
*Od teraz wymagamy, by wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

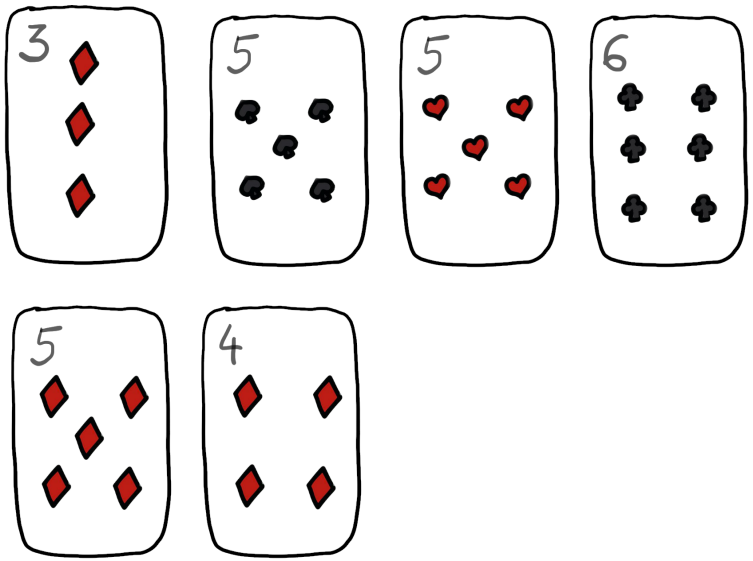
*Od teraz wymagamy, by wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

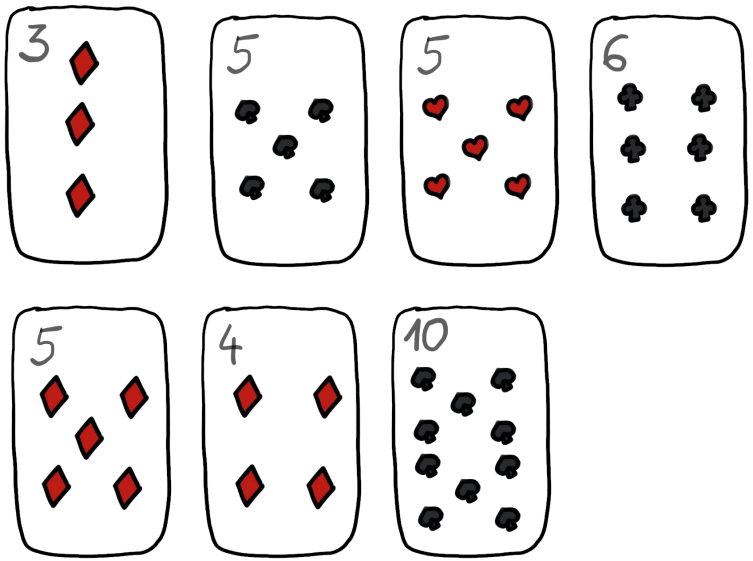
*Od teraz wymagamy, by wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

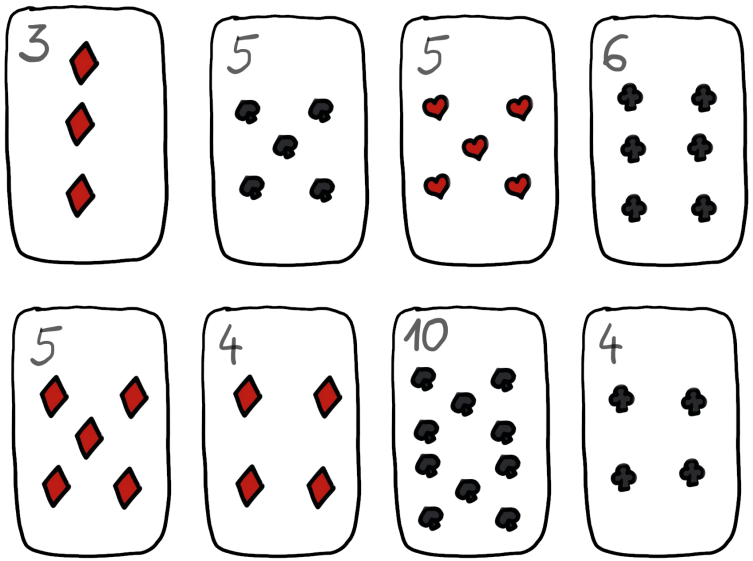
*Od teraz wymagamy, by wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

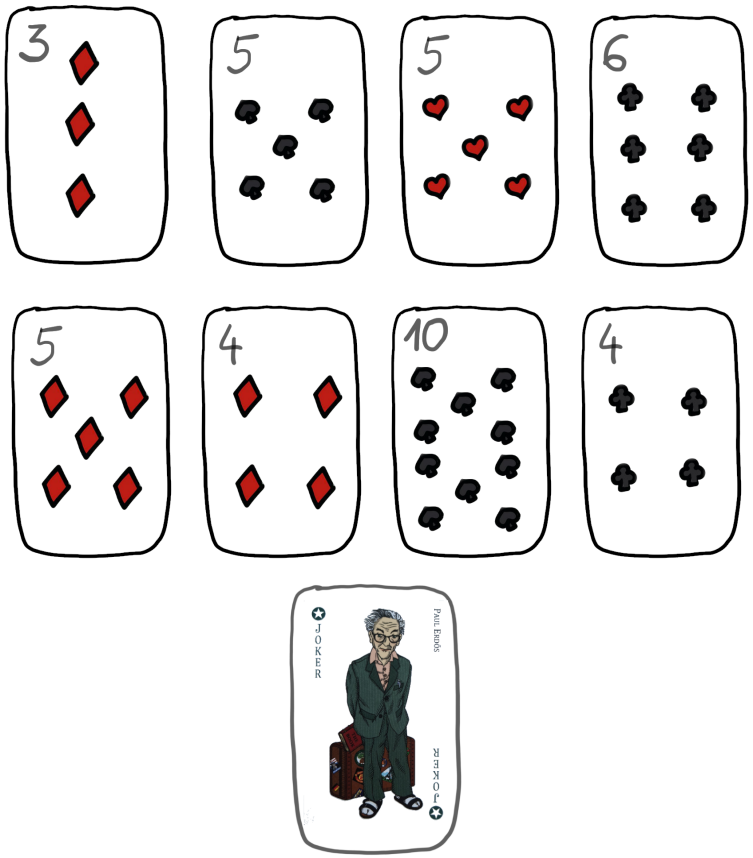
*Od teraz wymagamy, by wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

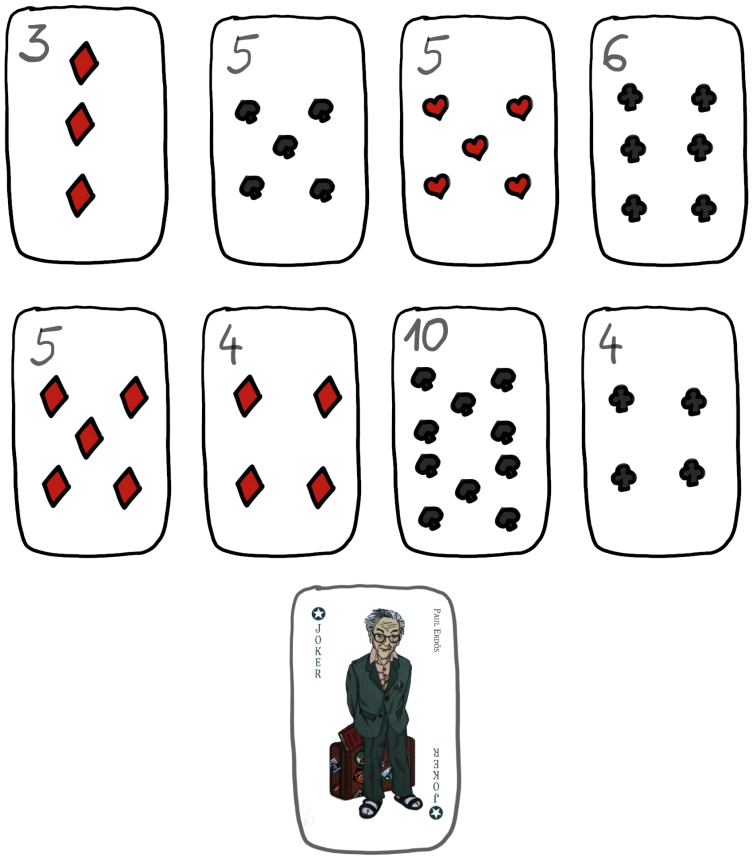
*Od teraz wymagamy, by wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



Utrudnijmy naszą grę!

Pytanie

*Od teraz wymagamy, by wskazać **6 kart** o sumie podzielnej przez 6. Czy ta gra musi się skończyć?*



$\mathbb{F}_p[x]$ i MTF

Niech $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ wraz z dodawaniem i mnożeniem modulo p.

Niech $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ wraz z dodawaniem i mnożeniem modulo p.

Definicja

$\mathbb{F}_p[x]$ – zbiór wielomianów zmiennej x o współczynnikach w $\mathbb{F}_p$.

Niech $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ wraz z dodawaniem i mnożeniem modulo p.

Definicja

$\mathbb{F}_p[x]$ – zbiór wielomianów zmiennej x o współczynnikach w $\mathbb{F}_p$.
$\mathbb{F}_p[x_1, \ldots, x_n]$ – wielomiany zmiennych $x_1, \ldots, x_n$ o współczynnikach w $\mathbb{F}_p$.

Niech $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ wraz z dodawaniem i mnożeniem modulo p.

Definicja

$\mathbb{F}_p[x]$ – zbiór wielomianów zmiennej x o współczynnikach w $\mathbb{F}_p$.
$\mathbb{F}_p[x_1, \ldots, x_n]$ – wielomiany zmiennych $x_1, \ldots, x_n$ o współczynnikach w $\mathbb{F}_p$.
Wielomian utożsamiamy z ciągiem jego współczynników!

Przykład:

Niech $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ wraz z dodawaniem i mnożeniem modulo p.

Definicja

$\mathbb{F}_p[x]$ – zbiór wielomianów zmiennej x o współczynnikach w $\mathbb{F}_p$.
$\mathbb{F}_p[x_1, \ldots, x_n]$ – wielomiany zmiennych $x_1, \ldots, x_n$ o współczynnikach w $\mathbb{F}_p$.
Wielomian utożsamiamy z ciągiem jego współczynników!

Przykład: w $\mathbb{F}_5[x]$:

$$(x^3 + 2x + 4) + (x^3 + 3x + 3) =$$

Niech $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ wraz z dodawaniem i mnożeniem modulo p.

Definicja

$\mathbb{F}_p[x]$ – zbiór wielomianów zmiennej x o współczynnikach w $\mathbb{F}_p$.
$\mathbb{F}_p[x_1, \ldots, x_n]$ – wielomiany zmiennych $x_1, \ldots, x_n$ o współczynnikach w $\mathbb{F}_p$.
Wielomian utożsamiamy z ciągiem jego współczynników!

Przykład: w $\mathbb{F}_5[x]$:

$$(x^3 + 2x + 4) + (x^3 + 3x + 3) = 2 \cdot x^3$$

Niech $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ wraz z dodawaniem i mnożeniem modulo p.

Definicja

$\mathbb{F}_p[x]$ – zbiór wielomianów zmiennej x o współczynnikach w $\mathbb{F}_p$.
$\mathbb{F}_p[x_1, \ldots, x_n]$ – wielomiany zmiennych $x_1, \ldots, x_n$ o współczynnikach w $\mathbb{F}_p$.
Wielomian utożsamiamy z ciągiem jego współczynników!

Przykład: w $\mathbb{F}_5[x]$:

$$(x^3 + 2x + 4) + (x^3 + 3x + 3) = 2 \cdot x^3 + 0 \cdot x$$

Niech $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ wraz z dodawaniem i mnożeniem modulo p.

Definicja

$\mathbb{F}_p[x]$ – zbiór wielomianów zmiennej x o współczynnikach w $\mathbb{F}_p$.
$\mathbb{F}_p[x_1, \ldots, x_n]$ – wielomiany zmiennych $x_1, \ldots, x_n$ o współczynnikach w $\mathbb{F}_p$.
Wielomian utożsamiamy z ciągiem jego współczynników!

Przykład: w $\mathbb{F}_5[x]$:

$$(x^3 + 2x + 4) + (x^3 + 3x + 3) = 2 \cdot x^3 + 0 \cdot x + 2$$

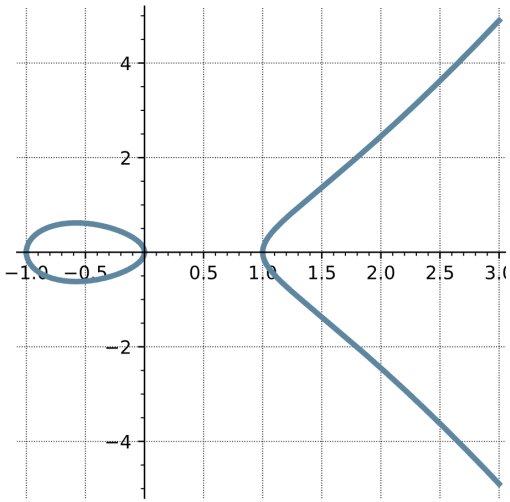
Niech $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ wraz z dodawaniem i mnożeniem modulo p.

Definicja

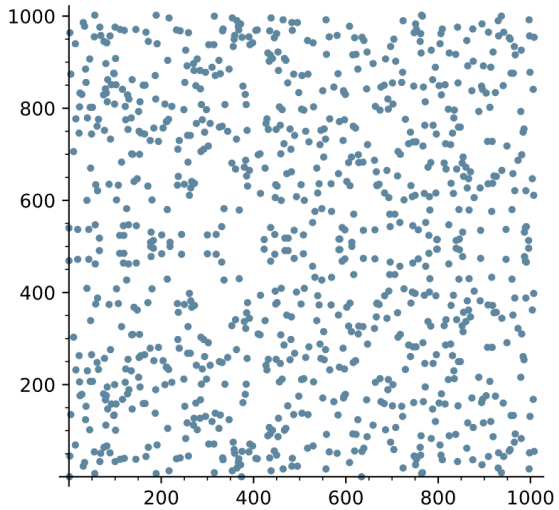
$\mathbb{F}_p[x]$ – zbiór wielomianów zmiennej x o współczynnikach w $\mathbb{F}_p$.
Wielomian utożsamiamy z ciągiem jego współczynników!

Dziedzina zajmująca się rozwiązaniami równań wielomianowych:

geometria algebraiczna



"Klasyczna" krzywa $y^2 = x^3 - x$



Krzywa $y^2 = x^3 - x$ modulo 1009

MTF, v1

Dla $a \in \mathbb{F}_p$ mamy: $a^p = a$.

MTF, v1

Dla $a \in \mathbb{F}_p$ mamy: $a^p = a$.

MTF, v2

Dla $a \in \mathbb{F}_p$ mamy: $a^{p-1} = \begin{cases} 1, & a \neq 0 \\ 0, & a = 0. \end{cases}$.

MTF, v1

Dla $a \in \mathbb{F}_p$ mamy: $a^p = a$.

MTF, v2

Dla $a \in \mathbb{F}_p$ mamy: $a^{p-1} = \begin{cases} 1, & a \neq 0 \\ 0, & a = 0. \end{cases}$.

Czy $x^p - x$ jest zatem wielomianem zerowym?

MTF, v1

Dla $a \in \mathbb{F}_p$ mamy: $a^p = a$.

MTF, v2

Dla $a \in \mathbb{F}_p$ mamy: $a^{p-1} = \begin{cases} 1, & a \neq 0 \\ 0, & a = 0. \end{cases}$.

Czy $x^p - x$ jest zatem wielomianem zerowym?

Nie, ale każdy element $\mathbb{F}_p$ jest jego pierwiastkiem:

$$x^p - x = (x - 0) \cdot (x - 1) \cdot \ldots \cdot (x - (p - 1)).$$

MTF, v1

Dla $a \in \mathbb{F}_p$ mamy: $a^p = a$.

MTF, v2

Dla $a \in \mathbb{F}_p$ mamy: $a^{p-1} = \begin{cases} 1, & a \neq 0 \\ 0, & a = 0. \end{cases}$.

Czy $x^p - x$ jest zatem wielomianem zerowym?

Nie, ale każdy element $\mathbb{F}_p$ jest jego pierwiastkiem:

$$x^p - x = (x - 0) \cdot (x - 1) \cdot \ldots \cdot (x - (p - 1)).$$

np. w $\mathbb{F}_3[x]$:

$$x^3 - x =$$

MTF, v1

Dla $a \in \mathbb{F}_p$ mamy: $a^p = a$.

MTF, v2

Dla $a \in \mathbb{F}_p$ mamy: $a^{p-1} = \begin{cases} 1, & a \neq 0 \\ 0, & a = 0. \end{cases}$.

Czy $x^p - x$ jest zatem wielomianem zerowym?
Nie, ale każdy element $\mathbb{F}_p$ jest jego pierwiastkiem:

$$x^p - x = (x - 0) \cdot (x - 1) \cdot \ldots \cdot (x - (p - 1)).$$

np. w $\mathbb{F}_3[x]$:

$$x^3 - x = x \cdot (x^2 - 1) =$$

MTF, v1

Dla $a \in \mathbb{F}_p$ mamy: $a^p = a$.

MTF, v2

Dla $a \in \mathbb{F}_p$ mamy: $a^{p-1} = \begin{cases} 1, & a \neq 0 \\ 0, & a = 0. \end{cases}$.

Czy $x^p - x$ jest zatem wielomianem zerowym?
Nie, ale każdy element $\mathbb{F}_p$ jest jego pierwiastkiem:

$$x^p - x = (x - 0) \cdot (x - 1) \cdot \ldots \cdot (x - (p - 1)).$$

np. w $\mathbb{F}_3[x]$:

$$x^3 - x = x \cdot (x^2 - 1) = x \cdot (x - 1) \cdot (x + 1) =$$

MTF, v1

Dla $a \in \mathbb{F}_p$ mamy: $a^p = a$.

MTF, v2

Dla $a \in \mathbb{F}_p$ mamy: $a^{p-1} = \begin{cases} 1, & a \neq 0 \\ 0, & a = 0. \end{cases}$.

Czy $x^p - x$ jest zatem wielomianem zerowym?
Nie, ale każdy element $\mathbb{F}_p$ jest jego pierwiastkiem:

$$x^p - x = (x - 0) \cdot (x - 1) \cdot \ldots \cdot (x - (p - 1)).$$

np. w $\mathbb{F}_3[x]$:

$$x^3 - x = x \cdot (x^2 - 1) = x \cdot (x - 1) \cdot (x + 1) = x \cdot (x - 1) \cdot (x - 2).$$

Twierdzenie Chevalley'a–Waringa.

CLAUDE CHEVALLEY

EDWARD WARING

Twierdzenie Chevalley'a–Warninga.

CLAUDE CHEVALLEY

Motywacja: jeżeli w jednorodnym układzie równań liniowych

$$\#\text{ zmiennych } > \#\text{ równań },$$

to istnieje niezerowe rozwiązanie!

Motywacja: jeżeli w jednorodnym układzie równań liniowych

$$\#\text{ zmiennych } > \#\text{ równań },$$

to istnieje niezerowe rozwiązanie!

Twierdzenie (Chevalley–Warning)

Niech $P_1, \ldots, P_r \in \mathbb{Z}[x_1, \ldots, x_n]$ *oraz*

$$\mathcal{Z} := \{t = (t_1, \ldots, t_n) \in \mathbb{F}_p^n : P_1(t) \equiv \ldots \equiv P_r(t) \equiv 0 \pmod{p}\}$$

Jeżeli $n > \deg P_1 + \ldots + \deg P_r$, *to* $p | \#\mathcal{Z}$.

Motywacja: jeżeli w jednorodnym układzie równań liniowych

$$\#\text{ zmiennych } > \#\text{ równań },$$

to istnieje niezerowe rozwiązanie!

Twierdzenie (Chevalley–Warning)

Niech $P_1, \ldots, P_r \in \mathbb{Z}[x_1, \ldots, x_n]$ *oraz*

$$\mathcal{Z} := \{t = (t_1, \ldots, t_n) \in \mathbb{F}_p^n : P_1(t) \equiv \ldots \equiv P_r(t) \equiv 0 \pmod{p}\}$$

Jeżeli $n > \deg P_1 + \ldots + \deg P_r$, *to* $p | \#\mathcal{Z}$.

Wniosek

Jeżeli dodatkowo wielomiany $P_1, \ldots, P_r$ *są jednorodne, to* $\mathcal{Z}$ *ma element różny od* $(0, 0, \ldots, 0)$.

Geometryczne spojrzenie:

Geometryczne spojrzenie:

- zbiór $\mathcal{Z}$ jest rozmaitością algebraiczną,

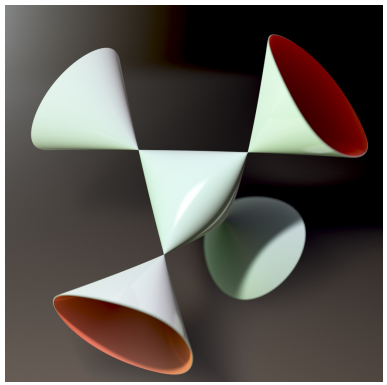
Geometryczne spojrzenie:

- zbiór $\mathcal{Z}$ jest rozmaitością algebraiczną,
- warunek $\deg P_1 + \ldots + \deg P_r < n$ oznacza, że $\mathcal{Z}$ jest rozmaitością Fano!

Geometryczne spojrzenie:

- zbiór $\mathcal{Z}$ jest rozmaitością algebraiczną,
- warunek $\deg P_1 + \ldots + \deg P_r < n$ oznacza, że $\mathcal{Z}$ jest rozmaitością Fano!

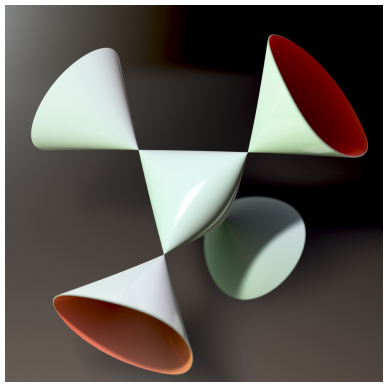
Rozmaitości Fano to jedna z podstawowych „cegiełek" w klasyfikacji rozmaitości algebraicznych. Intuicyjnie odpowiadają one rozmaitościom o dodatniej krzywiźnie.



Geometryczne spojrzenie:

- zbiór $\mathcal{Z}$ jest rozmaitością algebraiczną,
- warunek $\deg P_1 + \ldots + \deg P_r < n$ oznacza, że $\mathcal{Z}$ jest rozmaitością Fano!

Rozmaitości Fano to jedna z podstawowych „cegiełek" w klasyfikacji rozmaitości algebraicznych. Intuicyjnie odpowiadają one rozmaitościom o dodatniej krzywiźnie.



Hélène Esnault, 2003:
każda gładka rzutowa rozmaitość Fano nad $\mathbb{F}_p$ ma punkt wymierny!

Algebraiczne spojrzenie:

Algebra z dzieleniem to zbiór z działaniami $+, -, \cdot, \div$ (dozwalamy by mnożenie było nieprzemienne)

Algebraiczne spojrzenie:

Algebra z dzieleniem to zbiór z działaniami $+, -, \cdot, \div$ (dozwalamy by mnożenie było nieprzemienne) oraz mnożeniem przez „skalary” (elementy ustalonego ciała).

Algebraiczne spojrzenie:

Algebra z dzieleniem to zbiór z działaniami $+, -, \cdot, \div$ (dozwalamy by mnożenie było nieprzemienne) oraz mnożeniem przez „skalary” (elementy ustalonego ciała). **Centrum** algebry to elementy, które przy mnożeniu są przemienne ze wszystkimi innymi.

Algebraiczne spojrzenie:

Algebra z dzieleniem to zbiór z działaniami $+, -, \cdot, \div$ (dozwalamy by mnożenie było nieprzemienne) oraz mnożeniem przez „skalary" (elementy ustalonego ciała). **Centrum** algebry to elementy, które przy mnożeniu są przemienne ze wszystkimi innymi.

Przykład: kwaterniony

$$\mathbb{H} = \{a + b \cdot i + c \cdot j + d \cdot k : a, b, c, d \in \mathbb{R}\},$$

są algebrą z dzieleniem o centrum $\mathbb{R}$.

Algebraiczne spojrzenie:

Algebra z dzieleniem to zbiór z działaniami $+, -, \cdot, \div$ (dozwalamy by mnożenie było nieprzemienne) oraz mnożeniem przez „skalary" (elementy ustalonego ciała). **Centrum** algebry to elementy, które przy mnożeniu są przemienne ze wszystkimi innymi.

Przykład: kwaterniony

$$\mathbb{H} = \{a + b \cdot i + c \cdot j + d \cdot k : a, b, c, d \in \mathbb{R}\},$$

są algebrą z dzieleniem o centrum $\mathbb{R}$.

Z twierdzenia Chevalley'a–Warninga można wywnioskować, że jedyną algebrą z dzieleniem o centrum $\mathbb{F}_p$ jest $\mathbb{F}_p$.

$$\mathrm{Br}(\mathbb{R}) = \{\mathbb{R}, \mathbb{H}\}, \qquad \mathrm{Br}(\mathbb{F}_p) = \{\mathbb{F}_p\}.$$

Algebraiczne spojrzenie:

Algebra z dzieleniem to zbiór z działaniami $+, -, \cdot, \div$ (dozwalamy by mnożenie było nieprzemienne) oraz mnożeniem przez „skalary" (elementy ustalonego ciała). **Centrum** algebry to elementy, które przy mnożeniu są przemienne ze wszystkimi innymi.

Przykład: kwaterniony

$$\mathbb{H} = \{a + b \cdot i + c \cdot j + d \cdot k : a, b, c, d \in \mathbb{R}\},$$

są algebrą z dzieleniem o centrum $\mathbb{R}$.

Z twierdzenia Chevalley'a–Warninga można wywnioskować, że jedyną algebrą z dzieleniem o centrum $\mathbb{F}_p$ jest $\mathbb{F}_p$.

$$\mathrm{Br}(\mathbb{R}) = \{\mathbb{R}, \mathbb{H}\}, \qquad \mathrm{Br}(\mathbb{F}_p) = \{\mathbb{F}_p\}.$$

Zastosowanie nr 1: gra w nie-oczko.

Twierdzenie (Erdös, Ginzburg, Ziv, '61)

Jeżeli $a_1, a_2, \ldots \in \mathbb{Z}$, *to istnieje zbiór* $I \subset \{1, \ldots, 2n-1\}$ ***mocy*** n *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Twierdzenie (Erdös, Ginzburg, Ziv, '61)

*Jeżeli $a_1, a_2, \ldots \in \mathbb{Z}$, to istnieje zbiór $I \subset \{1, \ldots, 2n-1\}$ **mocy** n taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód dla $n = p$: korzystamy z twierdzenia CW dla wielomianów:

$$P_1(x_1, \ldots, x_{2p-1}) := a_1 x_1^{p-1} + \ldots + a_{2p-1} x_{2p-1}^{p-1}$$
$$P_2(x_1, \ldots, x_{2p-1}) := x_1^{p-1} + \ldots + x_{2p-1}^{p-1}$$

Twierdzenie (Erdös, Ginzburg, Ziv, '61)

Jeżeli $a_1, a_2, \ldots \in \mathbb{Z}$, *to istnieje zbiór* $I \subset \{1, \ldots, 2n-1\}$ ***mocy*** n *taki, że*

$$n \Big| \sum_{i \in I} a_i.$$

Twierdzenie (Erdös, Ginzburg, Ziv, '61)

Jeżeli $a_1, a_2, \ldots \in \mathbb{Z}$, *to istnieje zbiór* $I \subset \{1, \ldots, 2n-1\}$ ***mocy*** n *taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód dla $n = k \cdot m$**:**

Twierdzenie (Erdös, Ginzburg, Ziv, '61)

*Jeżeli $a_1, a_2, \ldots \in \mathbb{Z}$, to istnieje zbiór $I \subset \{1, \ldots, 2n-1\}$ **mocy** n taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód dla $n = k \cdot m$:

- założenie indukcyjne dla k: $I_1, \ldots, I_{2m-1} \subset \{1, \ldots, 2n-1\}$, parami rozłączne, takie że

$$k \mid \sum_{i \in I_j} a_i \qquad \text{dla } j = 1, \ldots, 2m-1.$$

Twierdzenie (Erdös, Ginzburg, Ziv, '61)

Jeżeli $a_1, a_2, \ldots \in \mathbb{Z}$, to istnieje zbiór $I \subset \{1, \ldots, 2n-1\}$ ***mocy*** *n taki, że*

$$n \mid \sum_{i \in I} a_i.$$

Dowód dla $n = k \cdot m$:

- założenie indukcyjne dla k: $I_1, \ldots, I_{2m-1} \subset \{1, \ldots, 2n-1\}$, parami rozłączne, takie że

$$k \mid \sum_{i \in I_j} a_i \qquad \text{dla } j = 1, \ldots, 2m-1.$$

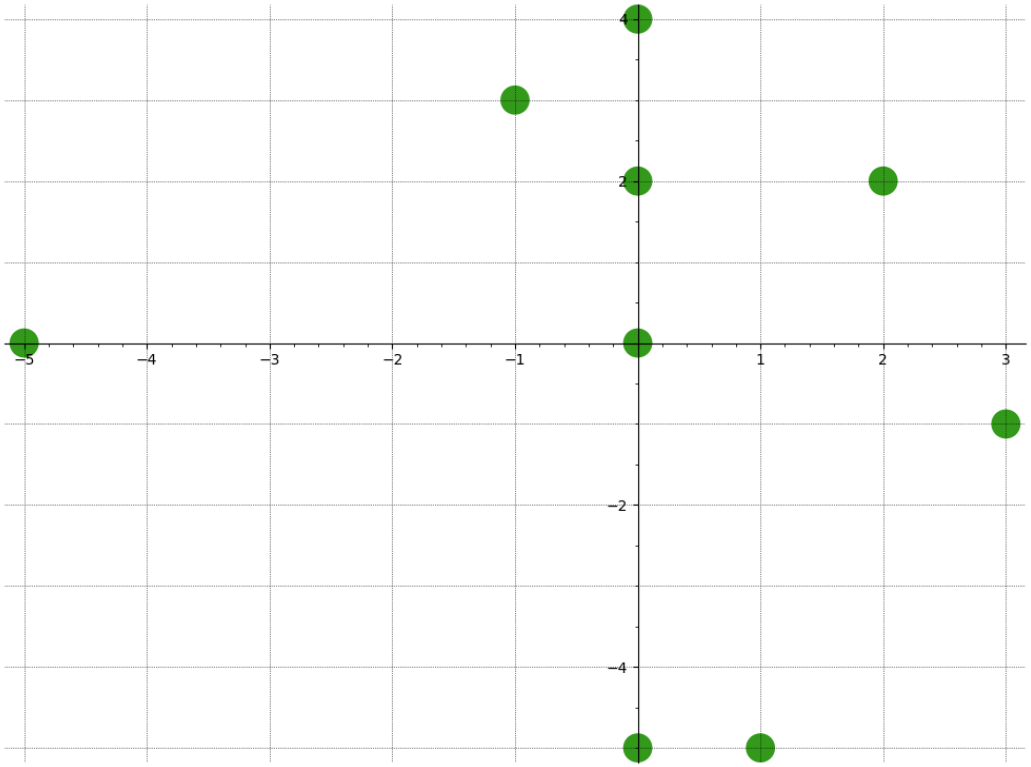
- założenie indukcyjne dla m oraz liczb:

$$b_j := \frac{1}{k} \sum_{i \in I_j} a_i, \qquad \text{dla } j = 1, \ldots, 2m-1$$

Zastosowanie nr 2: środek ciężkości.

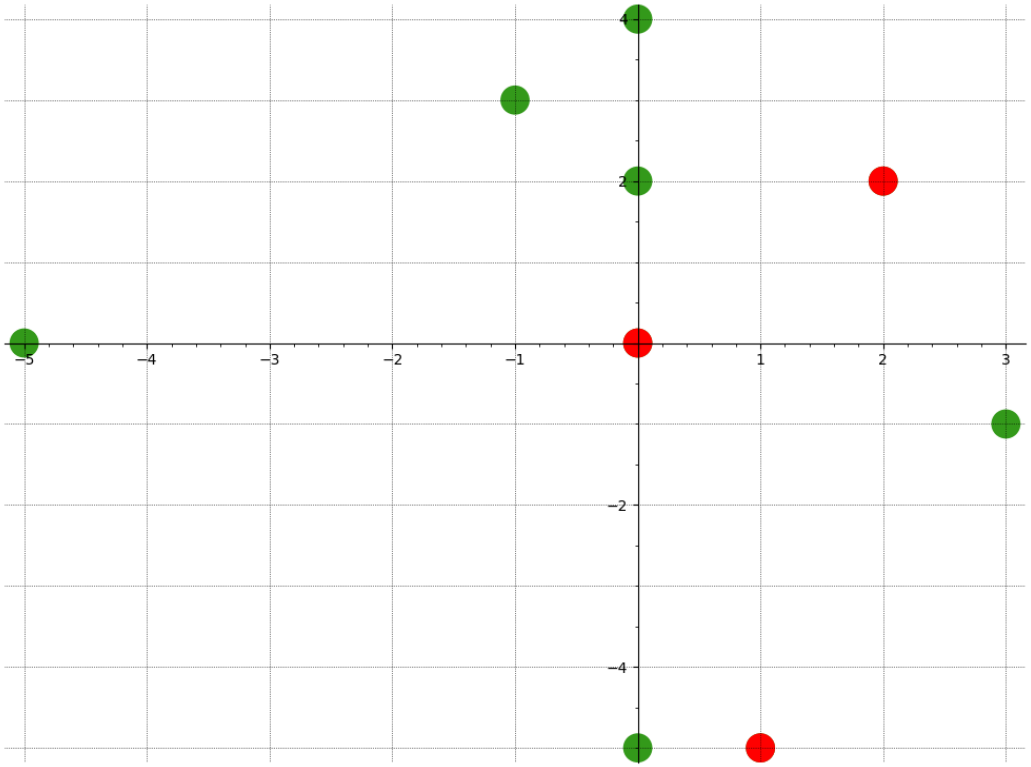
Twierdzenie

Dane jest $3 \cdot p$ punktów kratowych, których środkiem ciężkości jest punkt $(0, 0)$. Wówczas istnieje podzbiór p z nich, którego środkiem ciężkości jest punkt kratowy.



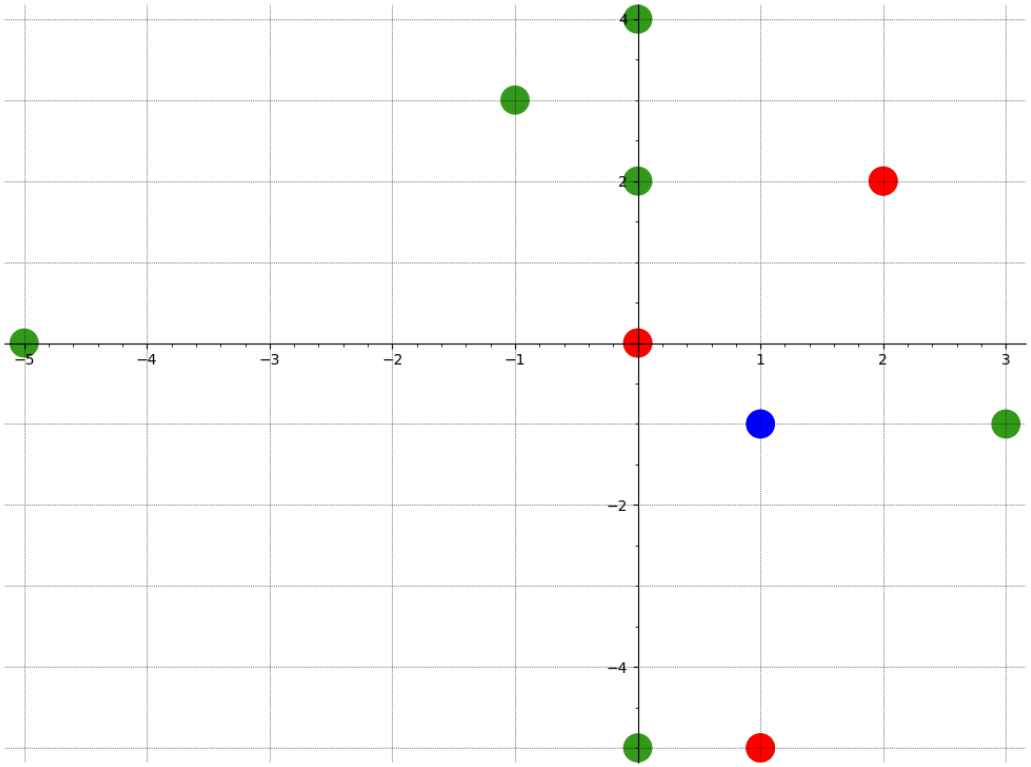
Twierdzenie

Dane jest $3 \cdot p$ punktów kratowych, których środkiem ciężkości jest punkt $(0, 0)$. Wówczas istnieje podzbiór p z nich, którego środkiem ciężkości jest punkt kratowy.



Twierdzenie

Dane jest $3 \cdot p$ punktów kratowych, których środkiem ciężkości jest punkt $(0, 0)$. Wówczas istnieje podzbiór p z nich, którego środkiem ciężkości jest punkt kratowy.



Twierdzenie

Dane jest $3 \cdot p$ punktów kratowych, których środkiem ciężkości jest punkt $(0, 0)$. Wówczas istnieje podzbiór p z nich, którego środkiem ciężkości jest punkt kratowy.

Dowód

Twierdzenie

Dane jest $3 \cdot p$ punktów kratowych, których środkiem ciężkości jest punkt $(0, 0)$. Wówczas istnieje podzbiór p z nich, którego środkiem ciężkości jest punkt kratowy.

Dowód

- *Punkty:* $(a_1, b_1), \ldots, (a_{3p}, b_{3p})$.

Twierdzenie

Dane jest $3 \cdot p$ punktów kratowych, których środkiem ciężkości jest punkt $(0, 0)$. Wówczas istnieje podzbiór p z nich, którego środkiem ciężkości jest punkt kratowy.

Dowód

- *Punkty:* $(a_1, b_1), \ldots, (a_{3p}, b_{3p})$.
- *Twierdzenie CW dla:*

$$P_1 := a_1 x_1^{p-1} + \ldots + a_{3p-1} x_{3p-1}^{p-1},$$
$$P_2 := b_1 x_1^{p-1} + \ldots + b_{3p-1} x_{3p-1}^{p-1},$$
$$P_3 := x_1^{p-1} + \ldots + x_{3p-1}^{p-1}.$$

Hipoteza Kemnitza

Dowolny zbiór $4p - 3$ punktów kratowych ma podzbiór mocy p, którego środek ciężkości jest również punktem kratowym.

Hipoteza Kemnitza

Dowolny zbiór $4p - 3$ punktów kratowych ma podzbiór mocy p, którego środek ciężkości jest również punktem kratowym.

- otwarta przez 20 lat,

Hipoteza Kemnitza

Dowolny zbiór $4p - 3$ punktów kratowych ma podzbiór mocy p, którego środek ciężkości jest również punktem kratowym.

- otwarta przez 20 lat,
- 2003: Reiher, – student, di Fiore – licealista.

Hipoteza Kemnitza

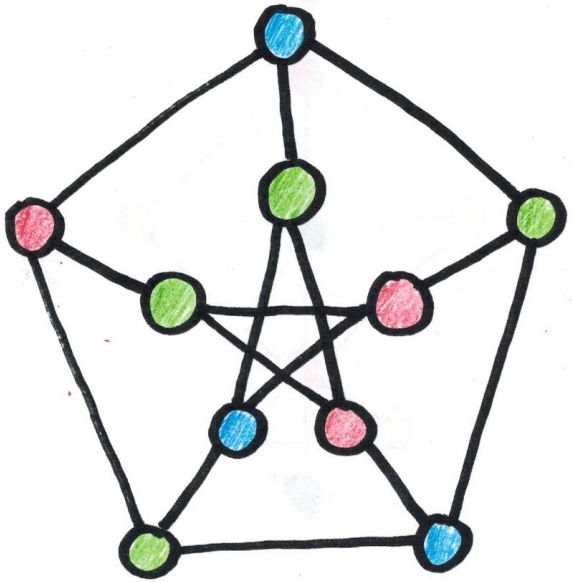
Dowolny zbiór $4p - 3$ punktów kratowych ma podzbiór mocy p, którego środek ciężkości jest również punktem kratowym.

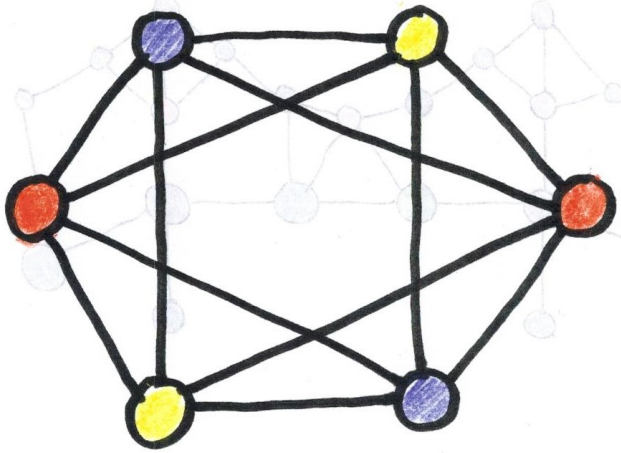
- otwarta przez 20 lat,
- 2003: Reiher, – student, di Fiore – licealista.

Pytanie

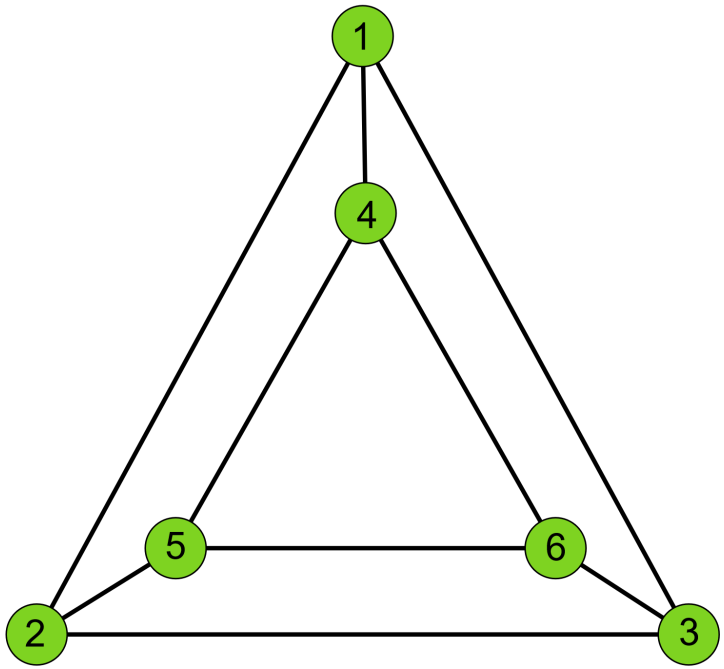
Co dla $(\mathbb{Z}/n)^k$, *gdzie* $k > 2$?

Zastosowanie nr 3: grafy regularne.

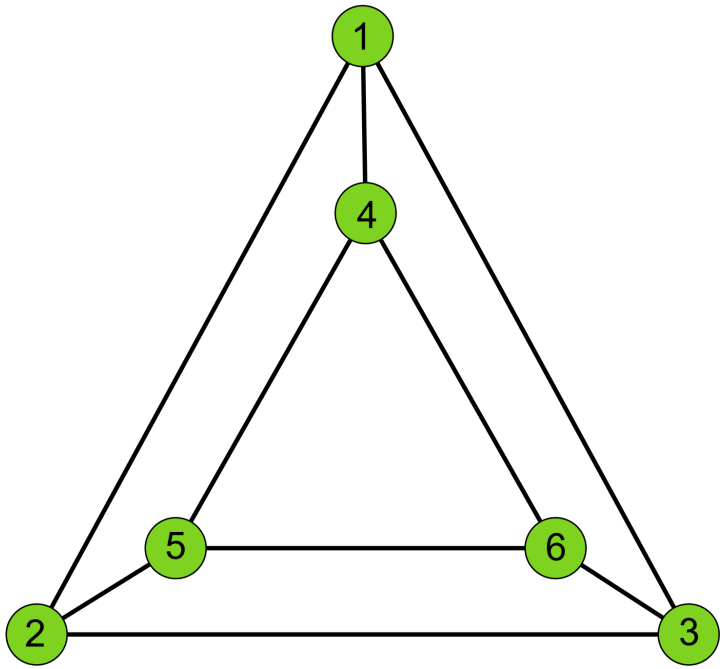




Graf k-regularny – z każdego wierzchołka wychodzi k-krawędzi.
Przykład – $k = 3$:



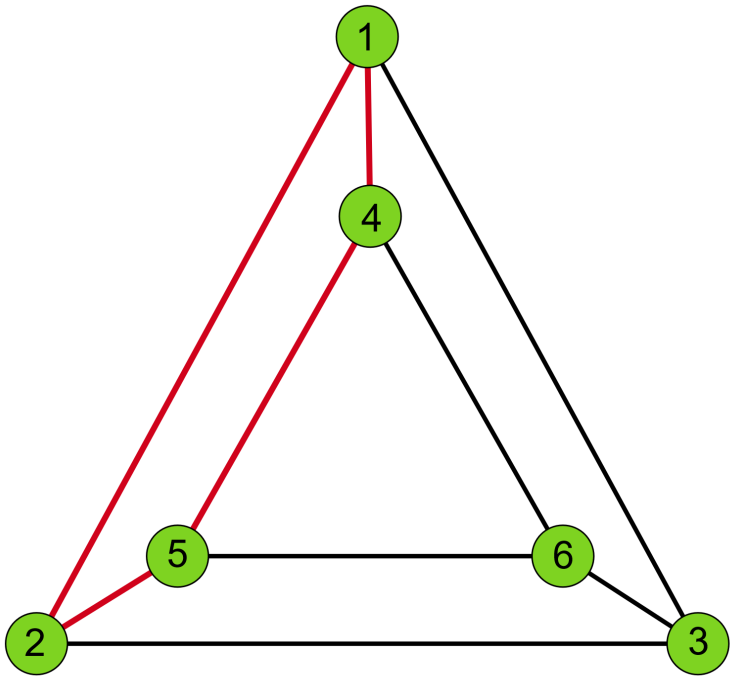
Graf k-regularny – z każdego wierzchołka wychodzi k-krawędzi.
Przykład – $k = 3$:



Twierdzenie

Dowolny $(2p-1)$-regularny graf ma spójny p-regularny podgraf.

Graf k-regularny – z każdego wierzchołka wychodzi k-krawędzi.
Przykład – $k = 3$:



Twierdzenie

Dowolny $(2p-1)$-regularny graf ma spójny p-regularny podgraf.

Twierdzenie

Dowolny $(2p-1)$-regularny graf ma spójny p-regularny podgraf.

Dowód:

Twierdzenie

Dowolny $(2p-1)$-regularny graf ma spójny p-regularny podgraf.

Dowód:

- krawędź $vw \in E \rightsquigarrow$ zmienna x_{vw},

Twierdzenie

Dowolny $(2p-1)$-regularny graf ma spójny p-regularny podgraf.

Dowód:

- krawędź $vw \in E \rightsquigarrow$ zmienna x_{vw},
- dla każdego wierzchołka $v \in V$ rozpatrujemy wielomian:

$$P_v(x) := \sum_{w:vw\in E} x_{vw}^{p-1}.$$

Twierdzenie

Dowolny $(2p-1)$-regularny graf ma spójny p-regularny podgraf.

Dowód:

- krawędź $vw \in E \rightsquigarrow$ zmienna x_{vw},
- dla każdego wierzchołka $v \in V$ rozpatrujemy wielomian:

$$P_v(x) := \sum_{w:vw \in E} x_{vw}^{p-1}.$$

Przykład: jak wygląda to dla grafu z poprzedniego slajdu?

Twierdzenie

Dowolny $(2p-1)$-regularny graf ma spójny p-regularny podgraf.

Dowód:

- krawędź $vw \in E \rightsquigarrow$ zmienna x_{vw},
- dla każdego wierzchołka $v \in V$ rozpatrujemy wielomian:

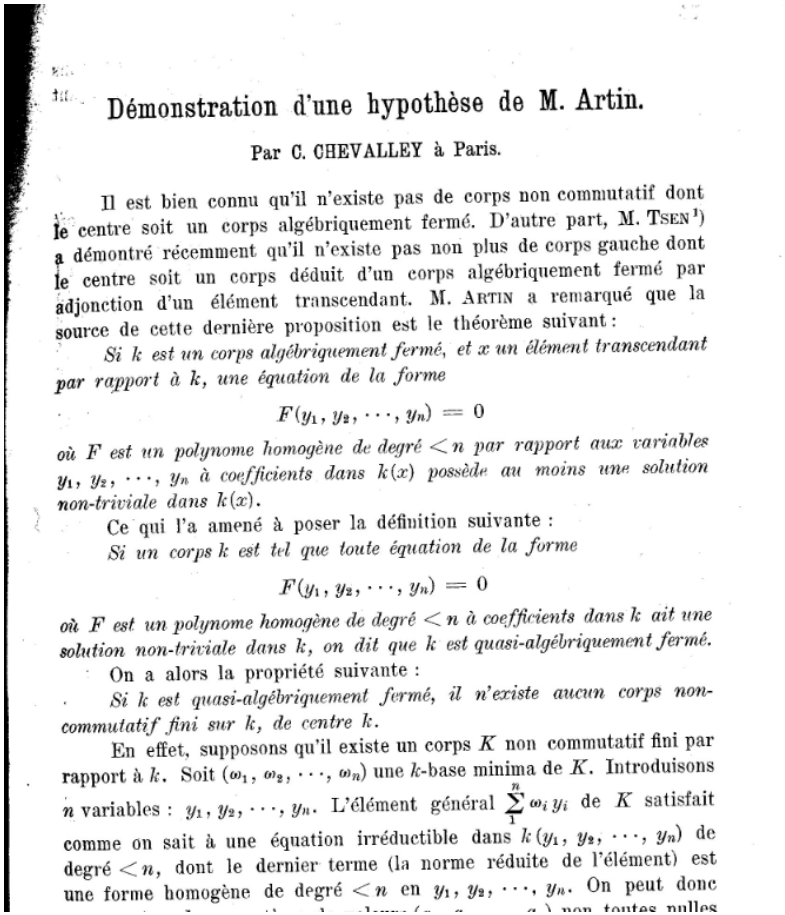
$$P_v(x) := \sum_{w:vw \in E} x_{vw}^{p-1}.$$

Przykład: jak wygląda to dla grafu z poprzedniego slajdu?

Pytanie

Co dla n złożonego?

Dowód twierdzenia Chevalley'a–Warninga



Démonstration d'une hypothèse de M. Artin.

Par C. CHEVALLEY à Paris.

Il est bien connu qu'il n'existe pas de corps non commutatif dont le centre soit un corps algébriquement fermé. D'autre part, M. TSEN[1]) a démontré récemment qu'il n'existe pas non plus de corps gauche dont le centre soit un corps déduit d'un corps algébriquement fermé par adjonction d'un élément transcendant. M. ARTIN a remarqué que la source de cette dernière proposition est le théorème suivant :

Si k est un corps algébriquement fermé, et x un élément transcendant par rapport à k, une équation de la forme

$$F(y_1, y_2, \cdots, y_n) = 0$$

où F est un polynome homogène de degré $< n$ par rapport aux variables $y_1, y_2, \cdots, y_n$ à coefficients dans $k(x)$ possède au moins une solution non-triviale dans $k(x)$.

Ce qui l'a amené à poser la définition suivante :

Si un corps k est tel que toute équation de la forme

$$F(y_1, y_2, \cdots, y_n) = 0$$

où F est un polynome homogène de degré $< n$ à coefficients dans k ait une solution non-triviale dans k, on dit que k est quasi-algébriquement fermé.

On a alors la propriété suivante :

Si k est quasi-algébriquement fermé, il n'existe aucun corps non-commutatif fini sur k, de centre k.

En effet, supposons qu'il existe un corps K non commutatif fini par rapport à k. Soit $(\omega_1, \omega_2, \cdots, \omega_n)$ une k-base minima de K. Introduisons n variables : $y_1, y_2, \cdots, y_n$. L'élément général $\sum_1^n \omega_i y_i$ de K satisfait comme on sait à une équation irréductible dans $k(y_1, y_2, \cdots, y_n)$ de degré $< n$, dont le dernier terme (la norme réduite de l'élément) est une forme homogène de degré $< n$ en $y_1, y_2, \cdots, y_n$. On peut donc

Twierdzenie (Chevalley–Warning)

Jeżeli $n > \deg P_1 + \ldots + \deg P_r$, *to*

$$p|\#\mathcal{Z} := \#\{t \in \mathbb{F}_p^n : P_1(t) \equiv \ldots \equiv P_r(t) \equiv 0 \pmod{p}\}.$$

Twierdzenie (Chevalley–Warning)

Jeżeli $n > \deg P_1 + \ldots + \deg P_r$, *to*

$$p|\#\mathcal{Z} := \#\{t \in \mathbb{F}_p^n : P_1(t) \equiv \ldots \equiv P_r(t) \equiv 0 \pmod{p}\}.$$

Lemat

$$\sum_{(t_1,\ldots,t_n)\in\mathbb{F}_p^n} t_1^{i_1} t_2^{i_2} \ldots t_n^{i_n} = \begin{cases} (-1)^n, & p-1|i_1,\ldots,i_n, \quad i_1,\ldots,i_n > 0, \\ 0, & w\ przeciwnym\ wypadku. \end{cases}$$

Slogan: *suma wszystkich wartości jednomianu jest zazwyczaj równa* 0.

Twierdzenie (Chevalley–Warning)

Jeżeli $n > \deg P_1 + \ldots + \deg P_r$, *to*

$$p|\#\mathcal{Z} := \#\{t \in \mathbb{F}_p^n : P_1(t) \equiv \ldots \equiv P_r(t) \equiv 0 \pmod{p}\}.$$

Lemat

$$\sum_{(t_1,\ldots,t_n)\in\mathbb{F}_p^n} t_1^{i_1} t_2^{i_2} \ldots t_n^{i_n} = \begin{cases} (-1)^n, & p-1|i_1,\ldots,i_n, \quad i_1,\ldots,i_n > 0, \\ 0, & w\ przeciwnym\ wypadku. \end{cases}$$

Slogan: *suma wszystkich wartości jednomianu jest zazwyczaj równa* 0.

$$\chi_{\mathcal{Z}}(t) \stackrel{\text{def}}{=} \begin{cases} 1, & t \in \mathcal{Z}, \\ 0, & t \notin \mathcal{Z}. \end{cases}$$

Twierdzenie (Chevalley–Warning)

Jeżeli $n > \deg P_1 + \ldots + \deg P_r$, *to*

$$p|\#\mathcal{Z} := \#\{t \in \mathbb{F}_p^n : P_1(t) \equiv \ldots \equiv P_r(t) \equiv 0 \pmod{p}\}.$$

Lemat

$$\sum_{(t_1,\ldots,t_n)\in\mathbb{F}_p^n} t_1^{i_1} t_2^{i_2} \ldots t_n^{i_n} = \begin{cases} (-1)^n, & p-1|i_1,\ldots,i_n, \quad i_1,\ldots,i_n > 0, \\ 0, & w\ przeciwnym\ wypadku. \end{cases}$$

Slogan: *suma wszystkich wartości jednomianu jest zazwyczaj równa* 0.

$$\chi_{\mathcal{Z}}(t) \stackrel{\text{def}}{=} \begin{cases} 1, & t \in \mathcal{Z}, \\ 0, & t \notin \mathcal{Z}. \end{cases} = (1-P_1(t)^{p-1})\cdot(1-P_2(t)^{p-1})\cdot\ldots\cdot(1-P_r(t)^{p-1}).$$

Dziękuję za uwagę!