POČÍTÁNÍ V $\mathbb{Z}_n$

$\mathbb{Z}$ věda o dělení se zbytkem $\rightarrow$ $a \mid b$ (relace „dělí")

$\downarrow$

kongruence modulo n (relace ekvivalence)

Def $a, b \in \mathbb{Z}$ a je kongruentní s b modulo n, když $n \mid (a, b)$

značíme $a \equiv b \pmod n$

Tvrzení: $a \equiv b \pmod n$ iff a má stejný zbytek po dělení n jako b

Tvrzení: $\equiv \pmod n$ je relace ekvivalence na $\mathbb{Z}$

Dk reflexivní $a \equiv a \pmod n$

~~symetrická když $a \equiv \pmod n$, pak $b \equiv$~~

symetrická když $a \equiv b \pmod n$, pak $b \equiv a \pmod n$

tranzitivní když $a \equiv b (\,)$ a $b \equiv c (\,)$, pak $a \equiv c (\,)$

} vzájemně

Důsledek: ekvivalence $\equiv \pmod n$ rozbije $\mathbb{Z}$ na třídy

$[a] = \{x \in \mathbb{Z},\ a \equiv x \pmod n\} =$

$= \{x \in \mathbb{Z},\ x = a + kn,\ k \in \mathbb{Z}\}$

liší se od a o násobek n

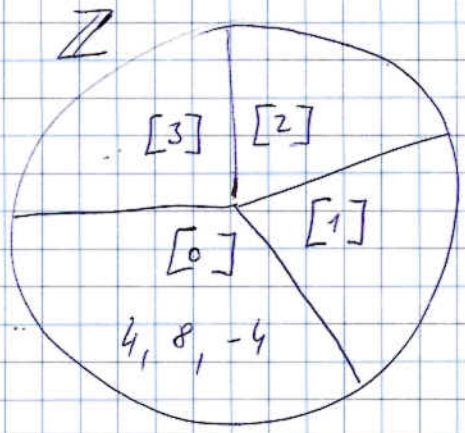
Množina všech tříd $\mathbb{Z}/_{\equiv (\mathrm{mod}\ n)} = \{[0], [1], \ldots, [n-1]\}$

zbytkové třídy modulo n
krátíme jednoduše $\mathbb{Z}_n$

Př $\equiv (\mathrm{mod}\ 4)$

$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$

$[1] = \{4k+1,\ k \in \mathbb{Z}\} = \{1, 5, 9 \ldots, -3, -7, \ldots\}$



Tvrzení: $\equiv (\mathrm{mod}\ n)$ se chová při sčítání a násobení

ANEB:

$a \equiv a_1 (\mathrm{mod}\ n)$, $b \equiv b_1 (\mathrm{mod}\ n)$

PAK:

$a + b \equiv a_1 + b_1 (\mathrm{mod}\ n)$

$a \cdot b \equiv a_1 \cdot b_1 (\mathrm{mod}\ n)$

Dk Když $a = kn + a_1$, $b = l \cdot n + b_1$

$a + b = (k+l)n + a_1 + b_1 \equiv a_1 + b_1 (\mathrm{mod}\ n)$

$a \cdot b = k \cdot l\, n^2 + b_1 \cdot kn + a_1 l \cdot n + a_1 b_1 (\mathrm{mod}\ n)$

Důležité: Mohu definovat sčítání $\oplus$ a násobení $\odot$ na třídách (v $\mathbb{Z}_n$)

$[a] \oplus [b] = [a+b]$

$[a] \odot [b] = [a \cdot b]$

Výsledek nezávisí na volbě reprezentanta.

$$\begin{array}{ccc} [a] \oplus [b] & = & [a+b] \\ \| & & \| \\ [a_1] \oplus [b_1] & = & [a_1+b_1] \end{array} \quad (=)$$

Pozn.: $\oplus, \odot$ je definováno přes reprezentanty $\Rightarrow$ každá příchozí vlastnost, která má $+, \cdot$ na $\mathbb{Z}$ (je to komutativní...)

Úmluva: ~~Budeme~~ Vynecháme $[\cdot], [\cdot]$ a $\oplus \odot$.

Budeme psát jednoduše

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

v $\mathbb{Z}_4$ $2+3=1$

místo: $[2] \oplus [3] = [5] = [1]$ v $\mathbb{Z}_4$

(PŘ) Kolik hodin bude za 3. 30 hodin od ~~tedy~~ teď, když je 13 hodin.

den má 24 hodin $\rightarrow$ modulo 24

$3.30 + 13 \equiv 3.6 + 13 \equiv 18 + 13 \equiv 31 \equiv 7 \pmod{24}$

$\rightarrow$ bude 7 hodin ráno.