**DMA Domácí koronaúkol č. 4b**

Tento úkol vypracujte a pak své řešení ukažte v rámci cvičení na MS Teams.

U obou následujících otázek rozhodněte, zda je dané tvrzení pravdivé či ne, a svou odpověď dokažte.
Pokud by nějaké tvrzení bylo nepravdivé, zkuste najít vhodnou podmínku, kterou by šlo přidat jako předpoklad a proměnit tak tvrzení v pravdivé. Snažte se o co nejobecnější tvrzení, přidaný předpoklad $x = y = c = 13$ by sice ledacos zachránil, ale není zrovna užitečný. Takové opravené tvrzení nemusíte dokazovat, náš obvyklý přístup přes algebru totiž skrývá zádrhel, ale borci to mohou zkusit. Nabízí se více cest.

**1.** Nechť $n \in \mathbb{N}$ a $x, y, c \in \mathbb{Z}$. Jestliže $x \equiv y \pmod{n}$, pak $cx \equiv cy \pmod{n}$.

**2.** Nechť $n \in \mathbb{N}$ a $x, y, c \in \mathbb{Z}$. Jestliže $cx \equiv cy \pmod{n}$, pak $x \equiv y \pmod{n}$.
Bonus pro drsně: Zkuste napsat důkaz opravené verze způsobem ze cvičení, kdy se začne $x =$, pak se něco provede a skončí se $= y$, a vystopovat všechny vlastnosti, které jsou třeba k správnosti takového výpočtu.

**Řešení:**

**1.** Platí.
Dk: Vezmeme $a, b$ libovolné $\in \mathbb{Z}$. Vyjdeme z předpokladu $x \equiv y \pmod{n}$:

$$\begin{aligned} y &= x + kn,\ k \in \mathbb{Z} \\ cy &= c(x + kn),\ k \in \mathbb{Z} \\ cy &= cx + (ck)n,\ ck \in \mathbb{Z} \end{aligned}$$

a proto $cx \equiv cy \pmod{n}$.

**2.** Poznámka: Tohle je už náročnější úkol, dávám to někdy u ústní zkoušky na A či náročné B. Proto jsem nepožadoval důkaz, jen rozmyšlení o platnosti. Ale k tomu je dobré se o ten důkaz alespoň pokusit.
Obvykle na takové věci chodíme přes algebru: $cx \equiv cy \pmod{n}$ dává $cy = cx + kn$.
Poznámka: $k$ je počet kroků nutných k posunu od $cx$ do $cy$, takže jej nemůžeme ovlivnit, například nelze si říct, že to vlastně je $ck$, aby to dál pomohlo.
Teď bychom rádi dělili číslem $c$, ale co když je to nula? (Vždy ve střehu!) To vypadá na pořádný průšvih, ale je to průšvih důkazu, nebo rovnou toho tvrzení? Trocha hraní ukáže, že tvrzení nefunguje. Pokud chceme dokázat, že obecné tvrzení (jsou v něm schovaná prokaždítka) neplatí, stačí jedno konkrétní selhání zvané protipříklad. Takže odpověď na danou otázku:
Tvrzení neplatí.
Dk: protipříklad: $c = 0$, $x = 3$, $y = 13$, $n = 4$, pak $cx \equiv cy \pmod{n}$ protože určitě $0 \equiv 0$ pro libovolné modulo, ale neplatí $3 \equiv 13 \pmod{4}$ neboť 4 nedělí $10 = 13 - 3$.

Pokus o opravu: Zkusíme přidat podmínku $c \neq 0$. Po vydělení dostaneme výraz, ve kterém je důležité osamostatnit velikost kroku $n$:

$$y = x + \frac{k}{c} \cdot n.$$

Rádi bychom napsali, že $\frac{k}{c} \in \mathbb{Z}$, ale nemůžeme, protože to nevíme. A to je další problém a velký. Celočíselnost je nutno vynutit, a to podmínkou, která pokud možno nepoužívá $k$, ale vychází z dat na vstupu. Najít tuto podmínku není v tomto typu důkazu snadné, lépe je vidět v alternativních důkazech. Něco ale přeci jen vycítit lze. Inspirace: Protože

$x, y$ jsou celé, je i $\frac{kn}{c}$ celé, tedy $c$ dělí $kn$. My ale chceme, aby $c$ dělilo $k$, proto mu musíme zakázat, aby bylo byť jen malým kouskem v $n$.
Opravené tvrzení:
Nechť $n \in \mathbb{N}$ a $x, y, c \in \mathbb{Z}$.

Jestliže $cx \equiv cy \pmod{n}$ a $\gcd(c, n) = 1$, pak $x \equiv y \pmod{n}$.

Důkaz 1: Z předpokladu máme $cy = cx + kn$ pro $k \in \mathbb{Z}$. Pak $kn = cy - cx$, tedy $c$ dělí $kn$. Ovšem $\gcd(c, n) = 1$, proto dle Euklidova lemmatu $c \mid k$, tedy $k = cm$ pro $m \in \mathbb{Z}$. Takže $cy = cx + cmn$. Také $c \neq 0$, jinak by $\gcd(c, n) = n$ (viz poznámka dole), a proto lze zkrátit, $y = x + mn$ pro $m \in \mathbb{Z}$ neboli $x \equiv y \pmod{n}$.

Důkaz 2: Z předpokladu $n$ dělí $cy - xy$. Tedy $n$ dělí $c(y - x)$, ale $\gcd(c, n) = 1$, tedy dle Euklidova lemmatu $n$ dělí $y - x$. Proto $x \equiv y \pmod{n}$.

Důkaz 3: Protože $\gcd(c, n) = 1$, má $c$ nějakou inverzi $d$ modulo $n$. Pokud na předpoklad $xc \equiv yc \pmod{n}$ aplikujeme první tvrzení s $d$, dostaneme $(xc)d \equiv (yc)d \pmod{n}$ neboli $x(cd) \equiv y(cd) \pmod{n}$. Ovšem $cd \equiv 1 \pmod{n}$, tedy $x \equiv y \pmod{n}$.

Důkaz 4: (bonus) Nechť $d$ je nějaké inverzní číslo k $c$ modulo $n$, dle $\gcd(c, n) = 1$ existuje. Pak

$$
\begin{aligned}
x &\equiv x \cdot 1 && \text{(existence jednotkového prvku)} \\
&\equiv x \cdot (cd) && \text{(existence inverzního prvku)} \\
&\equiv (xc)d && \text{(asociativní zákon)} \\
&\equiv (cx)d && \text{(komutativní zákon)} \\
&\equiv (cy)d && (cx \equiv cy \pmod{n}\text{, předpoklad z tvrzení}) \\
&\equiv (yc)d && \text{(komutativní zákon)} \\
&\equiv y(cd) && \text{(asociativní zákon)} \\
&\equiv y \cdot 1 \\
&\equiv y \pmod{n}.
\end{aligned}
$$

Poznámka: Algebraický důkaz obvykle funguje nejlépe. Tady je překvapivě ten nejkomplikovanější.

Poznámka: Pohled na rovnici $cy = cx + kn$ svádí k tomuto triku: Protože $gcd(c, n) = 1$, máme inverzi k $c$ modulo $n$, třeba $d$. Můžeme rovnici vynásobit: $dcy = dcx + dkn$. Bohužel, $dc = 1$ platí jen ve světě modula, ale ty rovnice jsou obyčejné, ve světě $\mathbb{Z}$, a součin $dc$ tedy může být cokoliv (kromě nuly). Například v $\mathbb{Z}_5$ je $2 \cdot 3 = 1$, tedy 3 je inverze k 2 modulo 5, ale ve světě $\mathbb{Z}$ je prostě $2 \cdot 3 = 6$. Míchat normální rovnice a svět modula tedy nefunguje.

Poznámka pro šťoury: Důkaz č. 1 není úplně korektní, protože podmínka $\gcd(c, n) = 1$ připouští $c = 0$, a to v případě, že $n = 1$. Ovšem ve světě modulo 1 jsou si všechna čísla rovna a to opravené tvrzení automaticky platí, takže správný a úplný důkaz by si případ $n = 1$ udělal bokem jako speciální případ. Popravdě řečeno, svět modula 1 je zvrhlík a spousta autorů takový modul ani nedovoluje, pak mají o starost méně.

Poznámka: Příklad 2 měl být pro vás výzvou, jak daleko se dostanete. Očekával jsem, že začnete s tou algebrou, a každý student by si měl všimnout problému s $c = 0$. Není snadné sledovat tyhle maličkosti, když se člověk soustředí na obtížnou matiku, ale je to nutné, protože často právě tyhle maličkosti pohřbí jinak ohromnou logickou stavbu. Pokud jste se dostali dál, je to skvělé.