Zadání cvičení pro 5. týden: 19.3.-23.3.

V pátém týdnu není teoretická přednáška. Pokračujte v procvičování modulární aritmetiky a modulárního umocňování, např- jako přípravu na RSA apod., ke kterým se dostaneme příští týden. Pokud už je vše procvičeno, můžete přímo na RSA přejít (zvláště ve skupinách, které přijdou o dva úterky v květnu).

Vysvětlete přiměřeně podrobně, jak se správně řešily úlohy z písemky.

Příklad. *(10.35)*
Pětice modulů 3; 5; 7; 11; 13 umožňuje jednoznačně reprezentovat čísla menší než jejich součin (tedy menší než 15015) a efektivně provádět (v případě potřeby distribuovaně) běžné aritmetické operace. Určete reprezentaci čísel 1234 a 5678 v této modulární soustavě a pomocí této reprezentace vypočtěte jejich součet a součin.)

Poznámka. Kromě jiného jde o pročvičení CRT.

Příklad. *(10.46)*
Ukažte, že jsou čísla $2^n - 1$*;* $2n$*;* $2^n + 1$ *po dvou nesoudělná a určete, kolik bitů mohou mít jimi určená čísla. Spočtěte reprezentaci čísla 118 v této soustavě s* $n = 3$*. Zapřemýšlejte o efeketivní realizaci této modulární aritmetiky.*

Poznámka. Reprezentace je $(6, 6, 1)$, jde rychle realizovat po blocích trojic bitů, viz. učebnice.

Další příklady na kongruence (lineární diofantické rovnice) a modulární umocňování (pokud možno zmiňte diskrétní logaritmus).