Zadání cvičení pro 2. týden: 26.2.-2.3.

Cílem cvičení je zvládat jednoduché úlohy zahrnující modulární aritmetiku. V úvodu si připomeňte rozklad přirozených čísel na součin prvočísel a počítání modulo zbytek (tj. kongruence).

Příklad. *(10.11)*

1. *Spočtěte* 7^{30} *modulo* 50 *(tj. hledejte zbytek po dělení číslem* 50*).*

2. *Určete dvě poslední cifry dekadického zápisu čísla* 7^{30}.

Příklad. *(10.12) Dokažte, že pro libovolné přirozené* n *je* $37^{n+2} + 16^{n+1} + 23^n$ *dělitelné sedmi.*

Příklad. *Spočtěte* 22^{-1} *modulo* 105.

Poznámka. Využijte Bezautovu rovnost. Buď zjistíte, že inverze neexistuje, nebo snadno spočtete. Zkuste poté využít rozklad $105 = 3 \cdot 5 \cdot 7$ a snadný výpočet modulo tyto tři faktory (teorii k tomu budeme mít časem také).

Pokud bude přebývat čas, spočtěte více příkladů na inverze.

Příklad. *(10.13) Dokažte, že číslo* $n = (835^5 + 6)^{18} - 1$ *je dělitelné číslem 112.*

Příklad. *(10.10) Dokažte, že jsou-li přirozená čísla* m, n *nesoudělná, jsou nesoudělná rovněž čísla* $m^2 + mn + n^2$ a $m^2 - mn + n^2$.

Poznámka. Předpokládejte soudělnost, tj. dělitelnost nějakým prvočíslem p, a doveďte do sporu.

Příklad. *Dokažte, že pro všechna přirozená* n *je číslo* $C_n = 4^{2n+1} - 10n - 4$ *dělitelné* 25.

Poznámka. Pomocí kongruencí lze velmi snadno ukázat, že je C_n dělitelné 5. Pak už nám zbude diskutovat jen 5 možných zbytků po dělení 25. Ještě jednodušší je použít indukci a pravidla pro modulární počítání.