**Domácí úkol do semináře z teorie čísel, 11. týden (28.11.2013)**

Nechť $p$ je liché prvočíslo. Cílem tohoto úkolu je dokázat, že pro libovolné $k \in \mathbb{Z}$, $k > 0$, je grupa $(\mathbb{Z}_{p^k}^\times, \cdot)$ cyklická. (Číslo $g \in \mathbb{Z}$ splňující $\langle [g]_{p^k} \rangle = \mathbb{Z}_{p^k}^\times$ se nazývá primitivní kořen modulo $p^k$.)

Dokažte následující tvrzení:

1. Pro libovolná $a, b, k \in \mathbb{Z}$, $k > 0$, platí
$$a \equiv b \pmod{p^k} \quad \Longrightarrow \quad a^p \equiv b^p \pmod{p^{k+1}}.$$
2. Grupa $(\mathbb{Z}_p^\times, \cdot)$ je cyklická.
3. Pro libovolné $c \in \mathbb{Z}$ splňující, že $\langle [c]_p \rangle = \mathbb{Z}_p^\times$ existuje $x \in \mathbb{Z}$ tak, že pro $g = c + px$ platí $g^{p-1} \equiv 1 + p \pmod{p^2}$.
4. Dokažte, že číslo $g$ získané výše splňuje pro každé $k \in \mathbb{Z}$, $k > 1$, kongruenci $g^{(p-1)p^{k-2}} \equiv 1 + p^{k-1} \pmod{p^k}$.
5. Dokažte, že číslo $g$ získané výše splňuje pro každé $k \in \mathbb{Z}$, $k > 0$, že zbytková třída $[g]_{p^k}$ je generátor grupy $\mathbb{Z}_{p^k}^\times$.

[Návod:
1. Rozložte $a^p - b^p$ na součin čísla $a - b$ a dalšího činitele, o kterém ukážete, že je dělitelný prvočíslem $p$.
2. Užijte větu o multiplikativních grupách konečných těles.
3. Umocněte $(c + px)^{p-1}$ binomickou větou a zjistěte, s čím je výsledek kongruentní modulo $p^2$. Vysvětlete, proč požadované $x \in \mathbb{Z}$ existuje.
4. Užijte indukci vzhledem ke $k$. Pravou stranu $(1 + p^{k-1})^p$ upravte binomickou větou modulo $p^{k+1}$.
5. Označte $n$ řád prvku $[g]_{p^k}$ v grupě $\mathbb{Z}_{p^k}^\times$. Ukažte, že $p - 1 \mid n$ a že $n \mid (p-1)p^{k-1}$. Vysvětlete, proč $n \nmid (p-1)p^{k-2}$.]