Domácí úkol z 8. října 2015

Zapište podrobně následující kroky v konstrukci p-adické Γ-funkce Γ_p ze semináře pro libovolné pevně zvolené prvočíslo p.

1. Předpokládejme, že prvočíslo $p \neq 2$.
   (a) Dokažte indukcí, že pro každé $n \in \mathbb{N}$ platí
   $$(1+p)^{p^{n-1}} \equiv 1 + p^n \pmod{p^{n+1}}.$$
   Užitím tohoto výsledku určete řád prvku $[1+p]_{p^n}$ v grupě $(\mathbb{Z}/p^n\mathbb{Z})^\times$.
   (b) Protože $(\mathbb{Z}/p\mathbb{Z})^\times$ je grupa jednotek konečného tělesa, je cyklická. Nechť $s \in \mathbb{Z}$ je zvoleno tak, že $[s]_p$ je generátor této grupy. Užitím (jediného existujícího) homomorfismu okruhů $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ odvoďte, že řád prvku $[s]_{p^n}$ v grupě $(\mathbb{Z}/p^n\mathbb{Z})^\times$ je dělitelný číslem $p-1$.
   (c) Pomocí vhodných vět z Algebry I ukažte, že grupa $(\mathbb{Z}/p^n\mathbb{Z})^\times$ je cyklická.
   (d) Odvoďte, že součin všech prvků grupy $(\mathbb{Z}/p^n\mathbb{Z})^\times$ je roven $[-1]_{p^n}$.
2. Nyní se zabývejme případem, kdy prvočíslo $p = 2$.
   (a) Dokažte indukcí, že pro každé $n \in \mathbb{N}$, $n \geq 2$, platí
   $$5^{2^{n-2}} \equiv 1 + 2^n \pmod{2^{n+1}}.$$
   Pomocí tohoto výsledku určete řád prvku $[5]_{2^n}$ v grupě $(\mathbb{Z}/2^n\mathbb{Z})^\times$.
   (b) Předpokládejme, že $n \geq 3$. Pomocí vhodných vět z Algebry I ukažte, že grupa $(\mathbb{Z}/2^n\mathbb{Z})^\times$ je součinem cyklické podgrupy generované prvkem $[5]_{2^n}$ a cyklické podgrupy generované prvkem $[-1]_{2^n}$.
   (c) Odvoďte, že v případě $n \geq 3$ je součin všech prvků grupy $(\mathbb{Z}/2^n\mathbb{Z})^\times$ roven $[1]_{2^n}$.
3. Nechť nadále je prvočíslo p libovolné. Pro libovolné $n \in \mathbb{N}$ definujme
   $$\Gamma_p(n) = (-1)^n \cdot \prod_{1 \leq i < n,\, p \nmid i} i.$$
   Dokažte, že tyto hodnoty je možné na okruhu $\mathbb{Z}_p$ všech celých p-adických čísel jednoznačně proložit spojitou funkci $\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p^\times$, kde $\mathbb{Z}_p^\times = \mathbb{Z}_p - p\mathbb{Z}_p$ je grupa jednotek okruhu $\mathbb{Z}_p$.