8. cvičení (5. dubna 2007)

Co jsme dělali?

Zabývali jsme se grupou $\mathbb{Z}_n^*$. Připomněli jsme si, co je to řád prvku a grupy a jak z Lagrangeovy věty vyplývá Eulerova věta. Pak jsme definovali involuci (prvek řádu 2) a primitivní prvek (prvek řádu $\varphi(n)$) modulo n a řekli si, že primitivní prvky existují, právě když $n = 2, 4, p^a, 2p^a$ (p je liché prvočíslo).

A ještě jsme se zmínili o tom, že polynom stupně n má nad tělesem $\mathbb{Z}_p$ nejvýše n kořenů, a definovali p-valuaci.

Příklady

-1. Dokaž, že 2 je primitivní prvek modulo 29.

0. Dokaž, že $x^{p-1} - 1 \equiv (x+1)(x+2)\cdots(x+p-1) \pmod{p}$ (p je prvočíslo).

1. Najdi všechny primitivní prvky modulo 19.

2. Vyřeš $x^3 \equiv 1 \pmod{1}9$.

3. V závislosti na $k \in \mathbb{N}$ a prvočíslu p spočti $1^k + 2^k + \cdots + (p-1)^k \pmod{p}$.

4. Kolik je primitivních prvků modulo n?

5. Urči všechny involuce v $\mathbb{Z}_{80}^*$.

6. Buď p prvočíslo. Dokaž, že má-li a řád 3 v $\mathbb{Z}_p^*$, má $1 + a$ řád 6 v $\mathbb{Z}_p^*$.

7. Vyřeš $1 + x + x^2 + \cdots + x^6 \equiv 0 \pmod{29}$.

8. Buď $p = 4t + 1$ prvočíslo. Dokaž, že a je primitivní prvek modulo p právě tehdy, když je $-a$ primitivní.

9. Dokaž, že součet všech přirozených čísel menších nebo rovných než n je $\frac{1}{2}n\varphi(n)$.

10. Dokaž, že součin všech primitivních prvků modulo prvočíslo p je kongruentní s $(-1)^{\varphi(p-1)} \pmod{p}$.

Těžší příklady

1. Buď p prvočíslo, $q \in \mathbb{Q}$. Urči hodnotu $v_p(q)$, znáš-li vyjádření čísla q v soustavě o základu p.

2. Dokaž, že je-li $2^n + 1 = p$ prvočíslo, je 3 primitivní prvek modulo p.