2. přednáška a cvičení (3. března 2009)

Co jsme dělali na přednášce?
Sekce 2.5, 2.11, 2.6 ze skript.

Co jsme dělali na cvičení?
Zabývali jsme se grupou $\mathbb{Z}_n^*$. Definovali jsme primitivní prvek (prvek řádu $\varphi(n)$). Grupa invertibilních prvků $\mathbb{Z}_p^*$, kde p je prvočíslo, je cyklická ($\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$), neboli v ní existuje primitivní prvek.

Dále jsme zkoumali polynomy a řešení kongruencí vyšších stupňů. Polynom stupně n nad tělesem (například $\mathbb{Z}_p$) má nejvýš n kořenů.

Pro $P \in \mathbb{Z}[x]$ platí $a \equiv b \pmod m \Rightarrow P(a) \equiv P(b) \pmod m$, čehož využíváme při zkoušení všech možných zbytků. Další vhodnou metodou řešení nelineárních kongruencí je najít nějaký primitivní prvek a využít izomorfismu $\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$.

Příklady

-1. Najdi všechny primitivní prvky modulo 29.

0. Najdi všechny kořeny polynomu $x^{21} - 3$ v $\mathbb{Z}_{29}$.

1. Najdi všechny primitivní prvky modulo 19.

2. Vyřeš kongruenci $x^4 \equiv 4 \pmod{19}$.

3. Mějme prvočíslo p. Kolik je primitivních prvků modulo p?

4. Kolik má polynom $x^2 - 1$ kořenů v $\mathbb{Z}_8$?

5. Buď p liché prvočíslo. Dokaž, že $|\{x^2 \pmod p, 1 \leq x \leq p-1\}| = (p-1)/2$.

6. Dokaž, že je-li a primitivní prvek modulo p, platí $a^{(p-1)/2} \equiv -1 \pmod p$.

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

8. Mějme $a \in \mathbb{Z}$, prvočíslo p a $n \in \mathbb{N}, 1 \leq n \leq p-1$, označme $D = (n, p-1)$. Uvažujme polynom $P(x) = x^n - a$. Dokažte, že

a) pokud je $D = 1$, má polynom P právě jeden kořen v $\mathbb{Z}_p$,

b) pokud je $D > 1$, má polynom P v $\mathbb{Z}_p$ buď 0 nebo D kořenů.