Cvičení 22. 3. 2012

Máme zadaný polynom $t(x)$ stupně k v $\mathbb{Z}_n$ a chceme znát kořeny. Pokud je n prvočíslo, tak víme, že $t(x)$ má nejvýše k kořenů (pro n složené to platit nemusí). Vždy ale platí $x \equiv y \pmod{n} \Rightarrow t(x) \equiv t(y) \pmod{n}$.

Jak řešit rovnici $x^k \equiv a \pmod{p}$ pro p prvočíslo? Můžeme zkoušet hodnoty a používat Eulerovu větu, ale je také možné najít a využít generátor (tzv. primitivní prvek) grupy $\mathbb{Z}_p^\star$ (viz příklad).

Pro kvadratickou rovnici v $\mathbb{Z}_p$, p prvočíslo můžeme použít postup podobný tomu v $\mathbb{R}$ a převést hledání kořene na hledání odmocniny z determinantu D (bude ukázáno). Ne vždy ovšem takové číslo existuje (viz kapitola o kvadratických reziduích příště).

Příklad 1. Najděte všechny kořeny polynomů:

1. $x^3 + 6$ v $\mathbb{Z}_{11}$
2. $x^{21} - 3$ v $\mathbb{Z}_{29}$
3. $x^4 - 4$ v $\mathbb{Z}_{19}$
4. $x^2 + 2x + 2$ v $\mathbb{Z}_7$
5. $2x^2 + 3x + 1$ v $\mathbb{Z}_{41}$

Příklad 2. Najděte n a polynom stupně 2, který má v $\mathbb{Z}_n$ aspoň tři různé kořeny.

Příklad 3. Dokažte, že pro každé p prvočíslo existuje polynom t_p stupně aspoň 1, který nemá v $\mathbb{Z}_p$ žádný kořen.

Příklad 4. Buď p prvočíslo. Kolik existuje:

1. prvků $\mathbb{Z}_p^\star$, které lze psát jako n^2 pro nějaké $n \in \mathbb{Z}_p^\star$,
2. primitivních prvků v grupě $\mathbb{Z}_p^\star$?