Cvičení 22. 3. 2012 – řešení

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 $\mathbb{Z}_{41}$

Řešení: Při hledání odmocnin budeme používat fakt, že grupa $\mathbb{Z}_p^\star$ je pro p prvočíslo konečně generovaná a je tedy isomorfní $\mathbb{Z}_{p-1}$. Najít nějaký generátor (primitivní prvek) $\mathbb{Z}_p^\star$ dá určitou práci, my se spokojíme s tím, že takový prvek uhodneme a ověříme, že má řád $p - 1$.

1. Řešíme vlastně rovnici
$$x^3 \equiv 5 \pmod{11}$$
Přitom $\mathbb{Z}_{11}^\star$ má primitivní prvek 2 (mocniny $1, 2, 4, 8, 5, 10, 9, 7, 3, 6$), tedy můžeme substituovat: $x = 2^y \pmod{11}$ a rovnici přepsat na $(2^y)^3 \equiv 2^4 \pmod{11}$. Protože řád 2 je 10, nastane rovnost právě tehdy, když $3y \equiv 4 \pmod{10}$.

   Nyní je potřeba určité opatrnosti; aby úpravy byly ekvivalentní, můžeme pronásobovat obě strany rovnice pouze čísly nesoudělnými s 10 (jinak dostaneme neekvivalentní úpravy a musíme provádět zkoušku). V našem případě $3 \cdot 7 \equiv 1 \pmod{10}$, tedy po vynásobení obou stran 7 (všimněte si, že vlastně aplikujeme automorfismus grupy $\mathbb{Z}_{10}$) máme rovnici
$$y \equiv 4 \cdot 7 \equiv 8 \pmod{10}$$
$$x \equiv 2^8 \equiv 3 \pmod{11}.$$
   Úpravy byly ekvivalentní, rovnice má tedy jediné řešení $x = 3$.

2. Začátek je podobný: Máme rovnici $x^{21} \equiv 3 \pmod{29}$. Evidentně $x \neq 0$. Grupa $\mathbb{Z}_{29}^\star$ má primitivní prvek 2 (posloupnost mocnin 1, 2, 4, 8, 16, 3, 6, 12, 24, 19, 9, 18, 7, 14, 28, 27, 25,...). Substituujeme $2^y = x$ a máme
$$2^{21y} \equiv 2^5 \pmod{29}.$$

Tedy

$$21y \equiv 5 \pmod{28}$$

Nyní levá strana této rovnice je dělitelná 7 stejně jako 28, tedy bychom museli mít $28|21y-5$, čili $7|21y-5$, čili $7|5$, což nejde. Polynom tedy nemá žádný kořen.

Funguje také postup vynásobení obou stran 4. Na cvičeních jsem byl vůči této úpravě opatrný, protože není ekvivalentní, ale byl jsem opatrný zbytečně: Pokud dokazujeme, že rovnice nemá řešení, tak nám stačí odvodit nepravdivé tvrzení. V našem případě:

$$84y \equiv 20 \pmod{28}$$

Přitom $84 \equiv 0 \pmod{28}$, tedy $0 \equiv 20 \pmod{28}$, což je spor.

3. Opět máme primitivní prvek 2. Tentokrát dostaneme po substituci $2^y = x$ rovnici

$$4y \equiv 2 \pmod{18}.$$

Nyní se nabízí vynásobit obě strany rovnice 9, ale tím dostaneme vždy pravdivé tvrzení $0 \equiv 0 \pmod{18}$, ačkoli naše rovnice určitě nemá za řešení všechna x. Budeme postupovat jinak: $18|4y-2$ je ekvivalentní $9|2y-1$ (lze „zkrátit dvojku“), takže jsme rovnici přepsali na

$$2y \equiv 1 \pmod{9},$$

což po vynásobení obou stran 5 dává $y \equiv 5 \pmod{9}$. Nyní přejdeme zpátky. V $\mathbb{Z}_{19}$ máme právě dvě čísla, co po vydělení 9 dají zbytek 5, $y = 5$ a $y = 14$. První dá $x_1 = 13$, druhé $x_2 = 6$, což jsou hledané kořeny (všimněte si, že $x_1 = -x_2 \pmod{19}$).

4. Upravíme rovnici jako běžnou kvadratickou rovnici:

$$\begin{aligned}(x+1)^2 + 1 &\pmod{0} \pmod{7}\\ (x+1)^2 &\pmod{6} \pmod{7}\end{aligned}$$

Vyzkoušením všech možností (nebo opět přes primitivní prvky, chcete-li) ale zjistíme, že 6 není kvadratický zbytek modulo 7, tedy rovnice nemá řešení.

5. Upravujeme jako výše (šlo by i dosadit do známého vzorečku pro kvadratickou rovnici). První úprava je vydělení 2 (tj. vynásobení 21):

$$\begin{aligned}2x^2 + 3x + 1 &\equiv 0 \pmod{41}\\ x^2 + 22x + 21 &\equiv 0 \pmod{41}\\ (x+11)^2 - 100 &\equiv 0 \pmod{41}\\ (x+11)^2 &\equiv 100 \pmod{41}\end{aligned}$$

Přitom odmocniny ze 100 jsou i v $\mathbb{Z}_{41}$ rovny ± 10. Tedy: $x + 11 \equiv \pm 10 \pmod 4$1 a máme dva kořeny $x_1 = 40$ a $x_2 = 20$.

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

Řešení: Vyhovuje například $x(x+1)$ v $\mathbb{Z}_6$. Ten má kořeny 0, 5 a 2.

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

Řešení: Volme $t_p(x) = 1 + \prod_{i=0}^{p-1}(x - i)$, to je polynom stupně p. Potom nutně $t_p(x) = 1$ pro každé $x \in \mathbb{Z}_p$.

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 $\mathbb{Z}_p^\star$?

Příklad 5. Pokud $p = 2$, tak je $\mathbb{Z}_p^\star$ triviální a odpověď je jedna a nula (pokud přistoupíme na to, že triviální grupa je nejmenší grupa obsahující prázdnou množinu).

Díky isomorfismu $\mathbb{Z}_p^\star$ a $\mathbb{Z}_{p-1}$ můžeme otázky pro $p > 2$ přepsat na problémy ve známější grupě $\mathbb{Z}_{p-1}$.

1. Hledáme velikost množiny $\{2x : x \in \mathbb{Z}_{p-1}\}$. Pro $n \in \mathbb{Z}_{p-1}$ je rovnice $2x \equiv n \pmod{p-1}$ řešitelná právě když n je sudé (protože $p-1$ je sudé. Takových prvků n je $(p-1)/2$, což je také odpověď.
2. Hledáme počet primitivních prvků grupy $\mathbb{Z}_{p-1}$. To jsou právě všechna čísla z $\{0, 1, \ldots, p-2\}$ nesoudělná s $p-1$, tedy $\phi(p-1)$ čísel.