Teorie čísel: Cvičení 5 – výsledky, nápovědy, vzorová řešení

Simona Hlavinková; email: simonkahlavinkova@gmail.com

Nápovědy:

0.,1. Postup byl předveden na cvičení. Lze vyjít přímo z definice, ale lepší je využít sblížené zlomky.

2.,3. Vyjděte přímo z definice.

4. a) Zřejmé. b) Není těžké si to rozmyslet přímo z definice. c) Vyžaduje to trochu přemýšlení, ale taky bych to odvozoval přímo z definice, ne z řetězových zlomků.

5. Tady podporuju použití kalkulačky.

6. Vcelku snadno to plyne z definice dobré aproximace.

8. Tuhle úlohu vůbec nechápu. Nechal jsem ji tu z loňska, ale netuším, jak je myšlená. Samozřejmě to okamžitě plyne z uvedené věty. Pokud máte pocit, že pointu cvičení chápete, určitě se mi ozvěte.

11. Cyklotomický polynom spočítejte podobně jako v předešlých příkladech rozkladem x^8-1 a využitím znalosti t_4, t_2 a t_1. Důkaz ireducibility není nijak zajímavý. Můžete přímo dokazovat nerozložitelnost v $\mathbb{Q}[x]$, nebo díky velmi užitečnému Gaussovu lemmatu stačí ověřit nerozložitelnost v $\mathbb{Z}[x]$. Polynom zjevně nemá racionální kořen (neboť nemá ani reálný) a přímým výpočtem lze ověřit, že neexistuje rozklad na dva racionální polynomy stupně 2.

Výsledky:

0. $\{0, \frac{1}{2}, \frac{2}{5}\}$, $\{2, \frac{5}{3}\}$.

1. $\{0, \frac{1}{3}, \frac{3}{10}\}$, $\{1, \frac{7}{8}\}$.

2. V prvním případě jen α, ve druhém $\lfloor\alpha\rfloor$, $\lceil\alpha\rceil$, α.

5. $\pi = [3, 7, 15, 1, \ldots]$, $\frac{3}{1}$, $\frac{22}{7}$, $\frac{333}{106}$, $\frac{355}{113}$.

9. $x^{14}-1 = t_1(x)t_2(x)t_7(x)t_{14}(x) = (x-1)(x+1)(x^6+x^5+x^4+x^3+x^2+x+1)(x^6-x^5+x^4-x^3+x^2-x+1)$; $x^{15}-1 = t_1(x)t_3(x)t_5(x)t_{15}(x) = (x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^8-x^7+x^5-x^4+x^3-x+1)$. Speciálně $t_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$ a $t_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$.

10. a) $x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$,
    b) $x^{12} - 1 = (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1)$.

11. Vyjde $x^4 + 1$. Nerozložitelnost se prostě ověří.

12. Použijte rozklad výrazu $a^p - 1$, dosaďte $a = x^{p^{k-1}}$, a postupujte např. indukcí.

13. Jedna možnost: Dokažte si následující lemma, z něhož už tvrzení snadno plyne: Pokud je n sudé, pak α je primitivní n-tá odmocnina z jedné právě tehdy, když je $-\alpha$ primitivní $2n$-tá odmocnina z jedné.
    Alternativa: Uvědomte si, že dělitelé $2n$ tvoří dvě skupiny: Dělitele n a dvojnásobky dělitelů n. Rozložte polynom $x^{2n} - 1$, zbavte se polynomů t_1 a t_2, a postupujte indukcí.