Zkoušený dostane pět úkolů sestavených z otázek a typů příkladů následujícího seznamu. Dva úkoly budou čistě teoretické (tedy primárně na pojmy a důkazy jejich vlastností) a tři kombinované s praktickou částí (zde půjde o pojmy, využití jejich vlastností k výpočtu, případně ilustrace (proti)příkladem) U teoretických otázek jsou uvedena čísla tvrzení podle skript, na něž míří (úlohy bez čísla míří jen na pojmy), Aplikační úlohy budou v testu samozřejmě číselně i ve své konkrétní formulaci obměněny.

1. Teoretické otázky

1.1. Vyslovte a dokažte horní odhad počtu prvočísel $\leq n$. (1.5)

1.2. Vyslovte a dokažte dolní odhad počtu prvočísel $\leq n$. (1.7)

1.3. Vyslovte a dokažte Bertrandův postulát. (1.3)

1.4. Co je Pellova rovnice a jak vypadá grupa všech jejích řešení? Své tvrzení dokažte. (2.1)

1.5. Co je Pellova rovnice? Dokažte, že existuje netriviálního řešení každé Pellovy rovnice. (2.3)

1.6. Co je řetězový zlomek a jak ho vyjádřit pomocí řetězových polynomů? Která čísla lze vyjádřit pomocí konečných řetězových zlomků? Své tvrzení dokažte. (2.4, 2.5)

1.7. Co jsou sblížené zlomky iracionálního čísla ξ? Vyslovte a dokažte jak konvergují k číslu ξ (2.9 (a)-(c)).

1.8. Definujte pojem dobrá aproximace a vyslovte a dokažte tvrzení o vztahu dobrých aproximací a sblížených zlomků (2.10)

1.9. Kdy je řetězový zlomek od nějakého členu řetězový? Své tvrzení dokažte. (2.13)

1.10. Jak najít řešení Pellovy rovnice pomocí sblížených zlomků? Své tvrzení dokažte. (2.14)

1.11. Charakterizujte prvočinitele v oboru Gaussových celých čísel a své tvrzení dokažte. (3.2)

1.12. Definujte pojem cyklotomický polynom a dokažte, že jde o polynomy s celočíselnými koeficienty. (3.5)

1.13. Dokažte, že je každý cyklotomický polynom ireducibilní nad $\mathbb{Q}$. (3.9)

1.14. Zaveďte pojem kvadratický zbytek a nezbytek. Co je Jacobiho symbol, jak ho spočítat pomocí mocnění a v jakém smyslu určuje grupový homomorfismus (4.1, 4.2)

1.15. Napište a dokažte, jak spočítat hodnoty $\left(\frac{-1}{p}\right)$ a $\left(\frac{2}{p}\right)$ v závislosti na hodnotě prvočísla p. (4.3, 4)

1.16. Definujte pojem charakteru a dokažte, že je grupa charakterů $X(\mathbb{Z}_p^*)$ pro prvočíslo p cyklická. (4.6)

1.17. Co je Gaussův součet a co kvadratický Gaussův součet charakteru? Určete velikost Gaussova součtu netriviálního charakteru a souvislost čtverce kvadratického Gaussova součtu a hodnoty $\left(\frac{-1}{p}\right)$. (4.8, 4.10)

1.18. Vyslovte a dokažte zákon kvadratické reciprocity. (4.11)

1.19. Co je Jakobiho symbol a jaké jsou jeho základní vlastnosti? (4.14)

1.20. Charakterizujte prvočinitele v oboru $\mathbb{Z}[\sqrt{-2}]$ a své tvrzení dokažte. (4.16)

1.21. Co je obecný pravděpodobnostní test prvočíselnosti? Uveďte nějaký příklad (bez důkazu).

1.22. Popište strukturu grupy $\mathbb{Z}_{p^n}^*$ pro liché prvočíslo p a své tvrzení dokažte. (5.5(a))

1.23. Popište strukturu grupy $\mathbb{Z}_{2^n}^*$ a své tvrzení dokažte. (5.5(b))

1.24. Popište Rabin-Millerův test prvočíselnosti a dokažte, že pro prvočíselný vstup je jeho podmínka splněna. Vysvětlete pojem silné pseudoprvočíslo (lhář) a svědek pro Rabin-Millerův test. (5.7)

1.25. Vysvětlete pojem míjení involuce a vyslovte a dokažte tvrzení o počtu prvků míjejících involucí v grupě $\prod_i \mathbb{Z}_{k^{k_i}}$. (5.12)

1.26. Vyslovte tvrzení o odhadu počtu svědků Rabin-Millerova testu a dokažte ho pro bezčtvercové N. (5.8)

1.27. Vyslovte tvrzení o odhadu počtu svědků Rabin-Millerova testu a dokažte ho pro N dělitelné čtvercem prvočísla. (5.8)

2. Aplikační úlohy

2.1. Pro všechna prvočísla p spočtěte $v_p(120)$.

2.2. Najděte příklad, kdy $v_p(a+b) > \max(v_p(a), v_p(b))$.

2.3. Určete hodnotu řetězového zlomku $[6, 7, 5]$.

2.4. Spočtěte řetězový zlomek pro číslo $\frac{12}{5}$.

2.5. Najděte posloupnost Fareyho zlomků řádu 6.

2.6. Určete řetězový zlomek a první tři sblížené zlomky čísla $\sqrt{2}$

2.7. Určete, kterému reálnému číslu odpovídá řetězový zlomek $[3, \overline{2, 1}]$.

2.8. Ukažte, že rovnice $x^2 - 3y^2 = -1$ nemá v $\mathbb{Z}$ řešení.

2.9. Víte-li, že $(x, y) = (3, 2)$ je řešení rovnice $x^2 - 2y^2 = 1$ v $\mathbb{Z}$ a najděte alespoň pět dalších řešení.

2.10. Víte-li, že $(x, y) = (3, 2)$ je řešení rovnice $x^2 - 2y^2 = 1$ v $\mathbb{Z}$ a najděte alespoň dvě dalších řešení splňující $x > 0 > y$.

2.11. Určete všechny dobré aproximace čísla $\frac{2}{5}$.

2.12. Rozložte polynom $x^{10} - 1$ na součin ireducibilních polynomů v $\mathbb{Q}[x]$.

2.13. Rozhodněte, zda je grupa charakterů $X(\mathbb{Z}_{50}^*)$ ($\mathbb{Z}_{15}^*$, $\mathbb{Z}_{61}^*$) cyklická.

2.14. Najděte ireducibilní rozklady čísla 15 v oboru Gaussový celých čísel $\mathbb{Z}[i]$.

2.15. Rozhodněte, zda existuje Gaussovo celá číslo s normou 39 (65).

2.16. Najděte všechny kvadratické zbytky modulo modulo 5.

2.17. Spočítejte hodnotu Legendreova symbolu $\left(\frac{17}{37}\right)$.

2.18. Určete všechny charaktery modulo 5.

2.19. Pro každý charakter modulo 5 spočtěte absolutní hodnotu jeho Gaussova součtu.

2.20. Pro všechny charaktery modulo 5 určete jejich řád v grupě $X(\mathbb{Z}_5^*)$.

2.21. Najděte všechny invertibilní prvky v oboru $\mathbb{Z}[\sqrt{-2}]$.

2.22. Určete hodnotu výrazu $\left(\frac{477}{247}\right)$.

2.23. Rozložte grupu $\mathbb{Z}_{240}^*$ na součin cyklických grup.

2.24. Najděte primitivní prvek modulo 81.

2.25. Které z grup $\mathbb{Z}_8^*$, $\mathbb{Z}_{81}^*$, $\mathbb{Z}_{18}^*$ jsou cyklické?

2.26. Vyřešte kongruenci $x^3 \equiv 1 \pmod{13}$.

2.27. Najděte všechny involuce v $\mathbb{Z}_{15}^*$ a rozhodněte, zda je tato grupa cyklická.

2.28. Najděte nějakého Rabin-Millerova lháře různého od 1 pro číslo 51.

2.29. Najděte nějakého nesoudělného Rabin-Millerova svědka pro číslo 51.