D smjer (Računarstvo i informacione tehnologije). **Programiranje II (četvrti semestar).** Ogledni primjeri pitanja za Završni ispit (30 poena). Dolazi jedno pitanje iz Algoritmi u teoriji brojeva i u kriptografiji + jedno pitanje iz Teorija NP–kompletnih zadataka + jedan zadatak.

Najvažnija pitanja su: teorija: 4, 9–22, zadaci: 4, 7–14.

⋈ Algoritmi u teoriji brojeva i u kriptografiji

1. Euklidov algoritam (za NZD – najveći zajednički djelilac) i njegova složenost. 2. Mala Fermaova teorema i njen dokaz. 3. Teorema o ostacima (Kineska teorema o ostacima) i njen dokaz. 4. Teorema na kojoj se temelji način RSA. Objasniti oznake. 5. Ukupna šema načina RSA. 6. Koliko vremena treba da se riješi zadatak "prime" (da li je dati broj prost) kada dati broj ima puno dekadnih cifara. 7. Na čemu se bazira sigurnost–zaštita u slučaju RSA načina. Koliko vremena treba da se dati broj rastavi na proste činioce. 8. Digitalni potpis, u slučaju kriptografskog sistema RSA. 9. Kriptografija pomoću javnog ključa: metoda kvadratnog ostatka – samo matematičke činjenice na kojima se sistem temelji, tj. dvije teoreme. Objasniti oznake. 10. Kriptografija pomoću javnog ključa: metoda kvadratnog ostatka – ukupni opis metode–sistema. 11. Ispitivanje primalnosti: Millerov postupak – šta je to pseudo–prost broj u nekoj bazi b i kako glasi algoritam. 12. Ispitivanje primalnosti: Miller–Rabinov postupak – šta je to jaki pseudo–prost broj u nekoj bazi b i kako glasi algoritam. 13. (Stream cipher) Sistem sa tajnim ključem – šta je to list za jednokratnu upotrebu ili engl. one–time pad. 14. (Stream cipher) Šta je to linear feedback shift register i opisati odgovarajući sistem sa tajnim ključem (tipa tajnog ključa). 15. U glavnim crtama o Prattovom sertifikatu primalnosti. 16. Alternativna definicija klase $\mathcal{NP}$ (gdje se vrši verifikacija).

⋈ Teorija NP–kompletnih zadataka

17. Pojam nedeterminističke Tjuringove mašine, jezika koji ona prihvata i njene vremenske složenosti. 18. Kako glasi zadatak o podjeli (partition problem). Skica njegovog rješenja pomoću nedeterminističke Tjuringove mašine. 19. Definisati dvije klase jezika (dvije klase zadataka) $\mathcal{P}$ i $\mathcal{NP}$. Kako glasi hipoteza, o njenom značaju. 20. Definisati klasu jezika (klasu zadataka) NPC. Prikazati na jednom crtežu tri važne klase u slučaju da je hipoteza o NP–kompletnosti tačna. 21. Razumna šema za kodiranje u slučaju zadatka o podjeli. U slučaju zadatka SAT. 22. Kako glasi zadatak SAT. Dokaz da je zadatak SAT NP–kompletan (Cookova teorema), u glavnim crtama. 23. Kako glasi zadatak o kliki. Dokaz da je zadatak o kliki NP–kompletan. 24. Neki zadaci za koje je dokazano da su teško rješivi.

⋈ Zadaci

Zadaci iz Obnavljanja

1. Neka je $n \geq 1$ i razmotrimo neusmjereni graf sa n vrhova. Koliko najviše ivica može da ima taj graf? Isto pitanje za usmjereni graf.

2. Neka je $n \geq 1$ i razmotrimo binarno drvo sa n vrhova. Kolika je najmanja moguća njegova visina. A kolika je najveća moguća.

3. Razmotrimo binarno drvo čija je visina $h = 10$. Koliki je najmanji mogući, odnosno najveći mogući broj vrhova. Isto pitanje za broj listova.

4. Nacrtati potpuno binarno drvo čija je visina $h = 2$ (ono ima $n = 7$ vrhova) i rasporediti brojeve $10, 20, \ldots, 70$ po vrhovima po prednjem redosljedu (preorder). To znači da treba da bude $\ell(v) \leq \ell(v_1) \leq \ell(v_2)$, gdje su v_1 i v_2 lijevi odnosno desni sin vrha v.

5. Nacrtati potpuno binarno drvo čija je visina $h = 2$ (ono ima $n = 7$ vrhova) i rasporediti brojeve $10, 20, \ldots, 70$ po vrhovima tako da važi inorder zakon (srednji redosljed). Treba da bude $\ell(v_1) \leq \ell(v) \leq \ell(v_2)$.

6. Nacrtati potpuno binarno drvo čija je visina $h = 3$ (ono ima $n = 15$ vrhova) i rasporediti po njegovim vrhovima na proizvoljan način slova $\mathrm{A}, \mathrm{B}, \ldots, \mathrm{O}$. Prikazati sve te podatke pomoću jednog niza. Ako je neki vrh na poziciji i u nizu onda su njegovi sinovi na pozicijama $2i$ i $2i+1$.

7. Nacrtati heap koji ima $n = 10$ vrhova i rasporediti brojeve $10, 20, \ldots, 100$ po njegovim vrhovima tako da važi $\ell(v) \geq \ell(v_1)$ i $\ell(v) \geq \ell(v_2)$, gdje su vrhovi v_1 i v_2 sinovi vrha v, kao što je uobičajeno za heap.

Zadaci iz Algoritmi u teoriji brojeva i u kriptografiji

8. Izračunati NZD$(2420, 196)$. Primijeniti Euklidov algoritam.

9. Koliko ima prostih brojeva do 1000 (približno)? A koliko do 10000? $\pi(x) \sim \frac{x}{\ln x}$.

10. Riješiti sistem jednačina: $x \bmod 7 = 2$, $x \bmod 15 = 3$ po nepoznatoj x $(0 \leq x \leq 104)$.

11. Naći bar jedno rješenje jednačine $7x - 6y = 16$, gdje se nepoznate x i y traže u skupu cijelih brojeva, ako rješenje postoji. Može se primijeniti uopšteni Euklidov algoritam.

12. Razmotrimo RSA kriptografski sistem: $p = 5$, $q = 7$, $n = pq = 35$, $\varphi(n) = (p-1)(q-1) = 24$, $e = 5$, $d = 5$. Neka poruka glasi $M = 20$. Izračunati kodirani oblik poruke $C = M^e \bmod n$. Zatim izračunati $C^d \bmod n$ (uvjeriti se da izlazi M). Ponoviti isti račun za još neko M $(1 < M < n)$.

13. Razmotrimo metodu kvadratnog ostatka: $p = 7$, $q = 11$, $n = pq = 77$. Neka poruka glasi $x = 15$ $(1 \leq x \leq n-1)$. Izračunati $y = x^2 \bmod n$, tj. izvršiti enkripciju. Da bismo se uvjerili da su formule za dekripciju pravilne, izračunati $y_1 = (y \bmod p)^{(p+1)/4} \bmod p$ i $y_2 = (y \bmod q)^{(q+1)/4} \bmod q$ i zatim vidjeti da važi $x \equiv \pm y_1 \,(\mathrm{mod}\, p)$, $x \equiv \pm y_2 \,(\mathrm{mod}\, q)$.

14. Razmotrimo metodu kvadratnog ostatka: $p = 7$, $q = 11$, $n = pq = 77$. Izabrati neku poruku x $(1 \leq x \leq n-1)$. Izračunati $y = x^2 \bmod n$. Izračunati $y_1 = (y \bmod p)^{(p+1)/4} \bmod p$ i $y_2 = (y \bmod q)^{(q+1)/4} \bmod q$. Naći sva rješenja sistema jednačina $x \equiv \pm y_1 \,(\mathrm{mod}\, p)$, $x \equiv \pm y_2 \,(\mathrm{mod}\, q)$ po nepoznatoj x, gdje je $1 \leq x \leq n-1$.

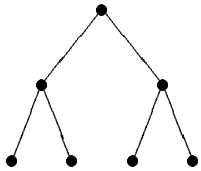
15. Ispitivanje primalnosti (da li je dati broj n prost). Razmotrimo Millerov postupak i $n = 91$. Za $b = 2$, da li važi $b^{n-1} \bmod n = 1$. Drugim riječima, uzimajući u obzir da je dati broj n složen, da li je dati broj pseudo–prost u bazi $b = 2$. Isto pitanje u slučaju baze $b = 3$.

16. Ispitivanje primalnosti (da li je dati broj n prost). Primijeniti Millerov postupak (test) na broj $n = 91$ po četiri baze ($b = 2$, $b = 3$, $b = 5$ i $b = 7$). Prolazi li n test?

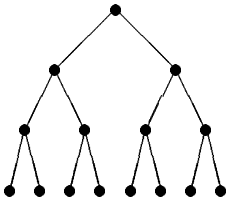
Zadaci iz Teorija NP–kompletnih zadataka

17. Uzmimo da je raspoloživo vrijeme računara, za rad programa, ograničeno na 1.000.000 taktova. Razmotrimo program P_1 čija je vremenska složenost (running time) $T(n) = n^2$ (složenost je polinomska) i drugi program P_2 čija je vremenska složenost $T(n) = 2^n$ (eksponencijalna funkcija). U slučaju P_1, za koje n, odnosno do kog najviše n program može da se izvrši. Isto pitanje za P_2.

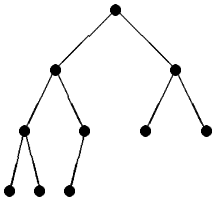
18. Uzmimo da nova vrsta računara ima deset puta veću učestanost, tako da je oslabljeno ranije ograničenje (1.000.000) na broj taktova i ono sada iznosi 10.000.000. Do kog najviše n je program mogao da se izvrši na staroj vrsti računara, odnosno do kog n može sada na boljem računaru. Uzeti da je vremenska složenost programa (koliko taktova treba da se program izvrši) jednaka $T(n) = n^2$. Isto pitanje ako je $T(n) = 2^n$.



potpuno binarno
drvo visine 2



potpuno binarno
drvo visine 3



heap sa 10 vrhova

Znamo da se prilikom sabiranja po modulu n može izvršiti redukcija pojedinog sabirka (djelimična redukcija ili potpuna redukcija), u smislu: dobiće se isti rezultat. Redukciju vršimo radi lakšeg računanja. Na primjer $(32+17) \bmod 10 = (22+17) \bmod 10$. Ili $(32+17) \bmod 10 = (2+17) \bmod 10$. Iste okolnosti važe prilikom množenja po nekom modulu: dozvoljeno je da se faktori redukuju. Na primjer $(37 \cdot 38) \bmod 11 = (4 \cdot 5) \bmod 11$.

Po definiciji, $x \bmod n$ je ostatak pri dijeljenju $x : n$. Na primjer $49 \bmod 20 = 9$. Na primjer $50 \bmod 20 = 10$. Po definiciji, $x_1 \equiv x_2 \,(\mathrm{mod}\, n)$ znači da se ostatak pri dijeljenju $x_1 : n$ poklapa sa ostatkom pri dijeljenju $x_2 : n$. Na primjer, relacija $68 \equiv 108 \,(\mathrm{mod}\, 20)$ je tačna. Na primjer, relacija $68 \equiv 118 \,(\mathrm{mod}\, 20)$ nije tačna.

Definicija. Neka je b prost broj. Neka je n složen broj. Ako je $b^{n-1} \equiv 1 \,(\mathrm{mod}\, n)$ onda se kaže da je broj n – pseudo–prost broj u bazi b. Definicija. Za neparan složen broj n kaže se da je jaki pseudo–prost broj u bazi $b \in \{2, 3, 5, 7, \ldots\}$ ako je $b^t \equiv 1 \,(\mathrm{mod}\, n)$ ili postoji r $(0 \leq r \leq s-1)$ takav da je $b^{2^r t} \equiv -1 \,(\mathrm{mod}\, n)$, gdje je $n - 1 = 2^s t$ i t je neparan.

Zadatak: $13a - 70b = 1$.

Rješenje pomoću uopštenog Euklidovog algoritma:
$\{70 : 13 = 5$ i ostaje $5\}$
$13a - 65b - 5b = 1$, $13(a - 5b) - 5b = 1$, smjena $a - 5b = c$, $13c - 5b = 1$,
$3c + 10c - 5b = 1$, $3c + 5(2c - b) = 1$, smjena $2c - b = d$, $3c + 5d = 1$,
$3c + 6d - d = 1$, $3(c + 2d) - d = 1$, smjena $c + 2d = e$, $3e - d = 1$,
sada jednačina ima oblik koef $\cdot$ nepoznata + koef $\cdot$ nepoznata = broj. Sada je jedan koef. $= \pm 1$. Zato se lako pronalazi jedno rješenje. Naime, vrijednost jedne nepoznate biramo proizvoljno (one čiji je koef. $\neq \pm 1$), npr. izaberemo da je ona 0. Dok vrijednost druge izračunamo iz tekućeg oblika jednačine. Nastavljamo od $3e - d = 1$. Izaberimo $e = 0$, slijedi $d = -1$, iz smjene imamo $c = 2$, iz smjene imamo $b = 5$, iz smjene imamo $a = 27$. Odgovor ako se traži jedno rješenje: $(a, b) = (27, 5)$. Dopuna: ako se a uveća za 70 a b za 13 onda nalazimo drugo rješenje $(a, b) = (97, 18)$ i slično.

Drugi primjer. Postavka zadatka: naći jedno rješenje jednačine $17x - 56y = 1$, gdje $(x, y) \in Z \times Z$. Treba primijeniti uopšteni Euklidov algoritam. Izrada: $17x - 56y = 1$, $17x - (3 \cdot 17 + 5)y = 1$, $17(x - 3y) - 5y = 1$, smjena $x - 3y = a$, $17a - 5y = 1$, $(3 \cdot 5 + 2)a - 5y = 1$, $5(3a - y) + 2a = 1$, smjena $3a - y = b$, $5b + 2a = 1$, $(2 \cdot 2 + 1)b + 2a = 1$, $2(2b + a) + b = 1$, smjena $2b + a = c$, $2c + b = 1$. Sada biramo proizvoljno $c \in Z$ [$\exists$ više rj, postoji ∞ rj]. Izaberimo $c = 0$. Tada iz $2c + b = 1$ imamo $b = 1$. Iz smjene $2b + a = c$ imamo $a = -2$. Slično, iz $3a - y = b$, $y = -7$. Dalje i najzad $x = -23$. Odgovor: jedno rješenje glasi $(x, y) = (-23, -7)$. [Ako je (x_0, y_0) rj onda je i $(x_0 + 56, y_0 + 17)$ rj i slično.]

Programiranje II, Popravni završni ispit
Djelimični spisak

1. Neka je $n \geq 1$ i razmotrimo binarno drvo sa n vrhova. Kolika je najmanja moguća njegova visina. A kolika je najveća moguća.

2. Nacrtati potpuno binarno drvo čija je visina $h = 2$ (ono ima $n = 7$ vrhova) i rasporediti brojeve $10, 20, \ldots, 70$ po vrhovima po prednjem redosljedu (preorder). U nastavku, rasporediti iste brojeve po vrhovima tako da važi inorder zakon (srednji redosljed).

3. Izračunati NZD$(2420, 392)$. Primijeniti Euklidov algoritam.

4. NZD$(2420, 784)$

5. Riješiti sistem jednačina $x \bmod 7 = 1$, $x \bmod 15 = 3$ po nepoznatoj x $(0 \leq x \leq 104)$.

6. $x \bmod 7 = 2$, $x \bmod 15 = 4$

7. Naći bar jedno rješenje jednačine $15x - 23y = 4$, gdje se nepoznate x i y traže u skupu cijelih brojeva, ako rješenje postoji. Može se primijeniti uopšteni Euklidov algoritam.

8. $15x - 23y = 8$

9. Neka je $e = 13$ i $n = 70$. Naći broj d $(1 \leq d \leq n - 1)$ da zadovoljava $de \equiv 1 \pmod{n}$, tzv. inverzni element. Uputstvo: $de = kn + 1$ za neko k.

10. $e = 17$ i $n = 130$

11. Razmotrimo RSA kriptografski sistem: $p = 3$, $q = 11$, $n = pq = 33$, $\varphi(n) = (p - 1)(q - 1) = 20$, $e = 3$, $d = 7$. Neka poruka glasi $M = 17$. Izračunati kodirani oblik poruke $C = M^e \bmod n$.

12. $M = 18$

13. Razmotrimo RSA kriptografski sistem: $p = 3$, $q = 11$, $n = pq = 33$, $\varphi(n) = (p - 1)(q - 1) = 20$, $e = 3$, $d = 7$. Neka poruka glasi $M = 19$. Izračunati kodirani oblik poruke $C = M^e \bmod n$. Zatim izračunati $C^d \bmod n$ (uvjeriti se da izlazi M).

14. $M = 20$

15. Razmotrimo metodu kvadratnog ostatka: $p = 7$, $q = 11$, $n = pq = 77$. Neka poruka glasi $x = 17$ $(1 \leq x \leq n - 1)$. Izračunati $y = x^2 \bmod n$, tj. izvršiti enkripciju.

16. $x = 19$

17. Razmotrimo metodu kvadratnog ostatka: $p = 7$, $q = 11$, $n = pq = 77$. Neka kodirani oblik poruke glasi $y = 25$. Želimo da izvršimo dekripciju. Naći broj x, gdje je $1 \leq x \leq n - 1$, takav da važi $y = x^2 \bmod n$. Uputstvo: $x = (\pm apy_2 \pm bqy_1) \bmod n$, gdje su a i b rješenja jednačine $ap + bq = 1$ (u razmatranom slučaju je $a = 8$ i $b = -5$) i gdje je $y_1 = y^{(p+1)/4} \bmod n$, $y_2 = y^{(q+1)/4} \bmod n$.

18. $y = 60$

19. Ispitivanje primalnosti (da li je dati broj n prost). Razmotrimo Millerov postupak i $n = 91$. Za $b = 2$, da li važi $b^{n-1} \bmod n = 1$. Drugim riječima, uzimajući u obzir da je dati broj n složen, da li je dati broj pseudo–prost u bazi $b = 2$.

20. $b = 3$ $\quad b = 3$

21. Kako glasi definicija jakog pseudo–prostog broja u određenoj bazi. Da li je broj $n = 45$ jaki pseudo–prost broj u bazi $b = 2$? Vidimo da je postavljeno pitanje povezano sa Miller–Rabinovim testom. Uputstvo: prikazati broj $n - 1$ u obliku $n - 1 = 2^s t$, izračunati brojeve $x_0, \ldots, x_s$ i vidjeti ima li niz $(x_0, \ldots, x_s)$ predviđeni oblik.

22. $n = 35$ $\quad$ u bazi $b = 3$

Iz teorije će doći samo oblasti: Algoritmi u teoriji brojeva i u kriptografiji i Teorija NP–kompletnih zadataka. Zadaci će doći navedenog tipa (isti kao navedeni ili sa drugim brojevima) uglavnom.