1 Uvodni zadaci

Zadatak 1.1 *Dokazati da* $6 \mid m(m^2+5)$ *važi za proizvoljan prirodan broj* m.

Zadatak 1.2 *Dokazati da* $30 \mid m^5 - m$ *važi za proizvoljan prirodan broj* m.

Zadatak 1.3 *Dokazati da* $30 \mid mn(m^4 - n^4)$ *važi za proizvoljne prirodne brojeve* m *i* n.

Zadatak 1.4 *Dokatati da* $42 \mid m^7 - m$ *važi za proizvoljan prirodan broj* m.

Zadatak 1.5 *Dokazati da* $2^m \mid (m+1)(m+2)\cdot\ldots\cdot(m+m)$ *važi za proizvoljan prirodan broj* m.

Zadatak 1.6 *Dokazati da je broj deljiv brojem 3 akko mu je zbir cifara deljiv brojem 3.*

Zadatak 1.7 *Dokazati da je* $NZD(a+b, a-b) \leq 2$ *ukoliko su* a *i* b *uzajamno prosti brojevi.*

Zadatak 1.8 *Dokazati da zbir kvadrata pet uzastopnih celih brojeva ne može biti potpuni kvadrat.*

Zadatak 1.9 *Koliko činilaca ima broj 945?*

2 Euklidov algoritam

Zadatak 2.1 *Izračunati najveći zajednički delilac datih brojeva, a zatim nzd predstaviti kao linearnu kombinaciju tih brojeva:*

a) 549 i 387

b) 589 i 343

Zadatak 2.2 *Izračunati:*

a) $160^{-1}(mod\ 841)$

b) $27^{-1}(mod\ 256)$

Zadatak 2.3 *Odraditi sva celobrojna rešenja jednačine* $53x + 47y = 1$.

Zadatak 2.4 *Odraditi sva celobrojna rešenja jednačine* $22x + 32y = 18$.

Zadatak 2.5 *Odrediti sve rešenja kongruencija:*

a) $3x \equiv 4(mod\ 7)$

b) $3x \equiv 4(mod\ 12)$

c) $9x \equiv 12(mod\ 21)$

d) $27x \equiv 25(mod\ 256)$

Zadatak 2.6 *Napisati Python funkciju koja određuje najveći zajednički delilac dva cela pozitivna broja.*

Zadatak 2.7 *Napisati Python funkciju koja određuje najveći zajednički delilac dva cela pozitivna broja i njihovu linearnu kombinaciju.*

Zadatak 2.8 *Napisati Python funkciju koja određuje multiplikativni inverz broja* a *po modulu* x.

3 Ojlerova funkcija

Zadatak 3.1 *Rastaviti na proste činioce brojeve 82798848 i 81057226635.*

Zadatak 3.2 *Rastaviti na proste činioce brojeve 10!, 15!, 20! i 30!.*

Zadatak 3.3 *Odrediti $\varphi(n)$ za svako $n \in [90, 100]$.*

Zadatak 3.4 *Odrediti $\varphi(n)$ za svako $n \in \{375, 720, 957, 988, 1200, 4320\}$.*

Zadatak 3.5 *Dokazati da je je broj p prost ako i samo ako $\varphi(p) = p - 1$.*

Zadatak 3.6 *Odrediti broj a ako je poznato da je $\varphi(a) = 120$, $a = p \cdot q$ i $p - q = 2$, pri čemu su p i q prosti brojevi.*

Zadatak 3.7 *Izračunati vrednost ostataka:*

a) $2^{1000000} (mod\ 7)$

b) $3^{23645} (mod\ 35)$

Zadatak 3.8 *Napisati Python funkciju koja faktoriše broj na proste činioce.*

Zadatak 3.9 *Napisati Python funkciju koja računa vrednost Ojlerove funkcije zadatog broja n.*

4 Stepenovanje kvadriranjem

Zadatak 4.1 *Izračunati vrednost sledećih izraza:*

a) $57^{1616} (mod\ 97)$

b) $11^{1536} (mod\ 105)$

c) $43^{257} (mod\ 59)$

Zadatak 4.2 *Neka je n proizvod različitih prostih brojeva takvih da za svaki prost broj p koji deli broj n važi $p - 1 \mid de - 1$, $d, e \in \mathbb{N}$. Dokazati da je $a^{de} \equiv a (mod\ n)$ za svako a, čak i ako je $NZD(a, n) > 1$.*

Zadatak 4.3 *Napisati funkciju koja izračunava $a^n (mod\ m)$ uzastopnim kvadriranjem.*

5 Konačna polja

Zadatak 5.1 *Napraviti tabelu indeksa po modulu 29 sa osnovom 2.*

Zadatak 5.2 *Napraviti tabelu indeksa po modulu 23 sa osnovom 2.*

Zadatak 5.3 *Napraviti tabelu indeksa po modulu 23 sa osnovom 5.*

Zadatak 5.4 *Odrediti x ako važi:*

a) $52^x \equiv 38 (mod\ 29)$

b) $23^x \equiv 9 (mod\ 29)$

c) $3^x \equiv 7 (mod\ 29)$

d) $3^x \equiv 6 (mod\ 23)$

Zadatak 5.5 *Odrediti sve generatore $\mathbb{Z}/n\mathbb{Z}^*$ za $n = 23$.*

Zadatak 5.6 *Odrediti sve generatore $\mathbb{Z}/n\mathbb{Z}^*$ za $n = 29$.*

Zadatak 5.7 *Izračunati:*

a) $5^{-1}(mod\ 29)$

b) $(-1)^{-1}(mod\ 23)$

Zadatak 5.8 *Odrediti sve nesvodljive polinome stepena* ≤ 3 *u* $\mathbb{F}_2[x]$.

Zadatak 5.9 *Da li je polinom* $x^4 + x^3 + x^2 + x + 1$ *nesvodljiv u* $\mathbb{F}_2[x]$*?*

Zadatak 5.10 *Napraviti tablicu množenja, tablicu inverza i proveriti da li je* x *generator u sledećim poljima:*

a) $\mathbb{F}_2[x]/(x^2 + x + 1)^*$

b) $\mathbb{F}_2[x]/(x^3 + x^2 + 1)^*$

Zadatak 5.11 *Napisati tablicu stepenova u* $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ *ako je* x *generator. Uz pomoć tablice izračunati* $(x^2 + 1)(x^2 + x + 1)$.

Zadatak 5.12 *Pomoću Euklidovog algoritma odrediti* $(x^4)^{-1}$ *u polju* $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$.

Zadatak 5.13 *Pomoću Euklidovog algoritma odrediti* $(x^4 + x^3 + 1)^{-1}$ *u polju* $\mathbb{F}_2[x]/(x^6 + x + 1)$.

6 SAES

Zadatak 6.1 *Odrediti matrice* A *i* B *takve da se druga komponenta preslikavanja* S *u algoritmu SAES može predstaviti u obliku* $AY + B$*, gde je* Y *vektor-kolona (nibl) dobijen iz prve komponenete* S.

Zadatak 6.2 *Odrediti tabelu* S *preslikavanja.*

Zadatak 6.3 *Primeniti proširivanje ključa na ključ "Qe".*

Zadatak 6.4 *Šifrovati otvoreni tekst "Ok" algoritmom SAES, ako je ključ "Qe".*

Zadatak 6.5 *Dešifrovati šifrat 0111 1101 1001 0100 algoritmom SAES, ako je ključ "Qe".*

Zadatak 6.6 *Napisati Python program koji omogućava enkripciju i dekripciju algortmom SAES.*

7 Sistemi sa javnim ključem

Zadatak 7.1 *Prikazati razmenu poruka u sistemu RSA ako je* $n = 697$, $p = 17$, $q = 41$, $d = 97$, $e = 33$, $M = 207$.

Zadatak 7.2 *Prikazati postupak Diffie-Helman protokola usaglašavanja ključa za* $q = 97$, $g = 5$, $a_A = 36$, $a_B = 58$ *tj. izračunati* g^{a_A}, g^{a_B} *i* K.

Zadatak 7.3 *Prikazati postupak El Gamal protokola za* $M = 30$, $q = 97$, $g = 5$, $a_B = 58$, $K = 17$.

Zadatak 7.4 *Prikazati postupak Massey-Omura razmene ključeva za* $q = 677$, $M = 470$, $e_A = 255$, $e_B = 421$.

Zadatak 7.5 *Napisati Python program koji implementara RSA algoritam.*

Zadatak 7.6 *Napisati Python program koji implementira Diffie-Helman protokol usaglašavanja ključa.*

Zadatak 7.7 *Napisati Python program koji implementira El Gamal protokol.*

Zadatak 7.8 *Napisati Python program koji implementira Massey-Omura protokol razmene ključeva.*

8 Eliptičke krive

Zadatak 8.1 *Za eliptičku krivu $E : y^2 = x^3 + 3x + 8$ nad poljem $\mathbb{F}_{13}$*

a) odrediti skup tačaka;

b) izračunati (1,8)+(9,7);

c) izračunati 2(9,7).

Zadatak 8.2 *Za eliptičku krivu $E : y^2 = x^3 + 3x + 8$ nad poljem F_{13}*

a) pokazati da je tačka $(1, 5)$ generator i napraviti tabelu umnožaka te tačke;

b) koristeći tabelu umnožaka izračunati:

- *(12,11)+(2,3),*
- *(12,2)+(9,6),*
- *25(9,7).*

Zadatak 8.3 *Dokazati da eliptička kriva nad poljem $\mathbb{F}_p$ ima najviše $2p + 1$ tačku.*

Zadatak 8.4 *Eliptička kriva koja se koristi za problem usaglašavanja ključeva Diffie-Helman protokola je $E : y^2 = x^3+3x+8$ nad poljem $\mathbb{F}_{13}$. Ako se koristi generator $G = (2, 3)$, tajni ključevi $e_A = 4$, $e_B = 5$, odrediti tačku koja se dobija kao rezultat usaglašavanja.*

Zadatak 8.5 *Za sistem El Gamal koristi se eliptička kriva $E : y^2 = x^3 + 3x + 8$ nad poljem $\mathbb{F}_{13}$. Generator je $G = (2, 3)$. Ako su tajni ključevi $e_A = 5$ i $e_B = 3$, prikazati postupak šifrovanja poruke $M = (12, 11)$ (koristi se slučajan broj $k = 4$), a zatim postupak dešifrovanja šifrata.*

Zadatak 8.6 *Napisati Python klasu koja opisuje tačku na eliptičkoj krivoj oblika $y^2 = x^3 + Ax + B$ i implementira sabiranje dve tačke, dupliranje tačke, negiranje tačke i višesturko sabiranje tačke.*

Zadatak 8.7 *Napisati Python klasu koja opisuje eliptičku krivu oblika $y^2 = x^3 + Ax + B$.*

Zadatak 8.8 *Napisati Python program koji implementira protokol usaglašavanja ključeva Diffie-Helman korišćenjem eliptičke krive.*

Zadatak 8.9 *Napisati Python program koji implementira El Gamal protokol nad eliptičkom krivom.*

9 Digitalni potpis

Zadatak 9.1 *U sistemu autentikacije zasnovanom na RSA korisnik A je izabrao javni ključ $e = 7$ i $n = 77$. Ako je on od korisnika B dobio broj $M = 23$, kako treba da glasi njegov odgovor da bi sagovornika ubedio u svoj identitet?*

Zadatak 9.2 *Za digitalne potpise zasnovane na sistemu RSA korisnici A i B imaju javne ključeve $e_A = 3$, $n_A = 15$ i $e_B = 7$, $n_B = 77$. Korisnik B želi da pošalje poruku $M = 4$ kao potpis nekog teksta. Koji ceo broj on treba da pošalje?*

Zadatak 9.3 *Dokazati da za digitalne potpise zasnovane na RSA važi sledeće tvrdjenje: Ako je S_1 potpis poruke m_1, a S_2 potpis poruke m_2, onda je S_1S_2 potpis poruke m_1m_2.*

Zadatak 9.4 *Opisati algoritam potpisivanja El Gamal za $p = 677$, $g = 2$, $S = 316$, $a_A = 307$, $k = 401$.*

10 Verižni razlomci

Zadatak 10.1 *Odrediti verižni razvoj datih brojeva i prvih 8 parcijalnih razlomaka:*

a) $\frac{107}{19}$

b) $\frac{7}{23}$

c) $\sqrt{3}$

d) $\sqrt{5}$

e) 1.625

f) π

Zadatak 10.2 *Dokazati da za svaki prirodan broj n važi $P_n \cdot Q_{n-1} - P_{n-1}Q_n = (-1)^{n-1}$.*

Zadatak 10.3 *Napisati Python funkciju za određivanje verižnog razvoja zadatog broja.*

Zadatak 10.4 *Napisati Python funkciju za određivanje vrednosti parcijalnog razlomka na osnovu verižnog razvoja.*

11 Linearni pomerački registar

Zadatak 11.1 *Odrediti orbite za $n = 3$, $(b_0, b_1, b_2) = (1, 1, 0)$, $(k_0, k_1, k_2) = (0, 1, 1)$.*

Zadatak 11.2 *Odrediti orbite za $n = 4$, $(b_0, b_1, b_2, b_3) = (1, 0, 1, 0)$, $(k_0, k_1, k_2, k_3) = (0, 1, 1, 1)$.*

Zadatak 11.3 *Odrediti orbite za $n = 4$, $(b_0, b_1, b_2, b_3) = (1, 0, 0, 1)$, $(k_0, k_1, k_2, k_3) = (0, 1, 1, 1)$.*

Zadatak 11.4 *Odrediti orbite za polinome:*

a) $1 + x^2 + x^3 + x^4$

b) $1 + x + x^5$

c) $1 + x + x^6$

d) $1 + x^3 + x^5$

Zadatak 11.5 *Odrediti povratne sprege i linearne pomeračke registre na osnovu otvorenog teksta $OT = [4, 0] = [00100, 00000]$ i šifrovanog teksta $ST = [17, 30] = [10001, 11110]$.*

Zadatak 11.6 *Napisati Python funkciju za određivanje $\boldsymbol{d}$ bitova ključa koji se dobija linearnim pomeračkim registrom sa povratnom spregom $\boldsymbol{b}$ počevši iz stanja $\boldsymbol{s}$.*

12 Slučajno lutanje

Zadatak 12.1 *Algoritmom slučajnog lutanja faktorisati sledeće brojeve ako se koristi $f(x) = x^2 + 1 (mod\ n)$ i $a_0 = 0$:*

a) 1357

b) 14873

Zadatak 12.2 *Odrediti n tako da je $Q(5, 98) = n \cdot G$ algoritmom slučajnog lutanja, ako je data eliptička kriva $E : y^2 = x^3 + 17x + 1$ u polju F_{101}, gde je $G(0, 1)$ generator i važi $103 \cdot G = \varnothing$.*

Zadatak 12.3 *Ako se zna da je $g = 2$ generator za F_{101}, odrediti x tako da je $y = 86 = g^x$ primenom algoritma lutanja kroz F_{101}.*

Zadatak 12.4 *Napisati Python funkciju za faktorizaciju broja $\boldsymbol{n}$ algoritmom slučajnog lutanja.*

13 Faktorizacija

Zadatak 13.1 *Primeniti Fermaovu faktorizaciju na sledeće brojeve:*

a) $n = 3229799$

b) $n = 1357$

c) $n = 21079$

Zadatak 13.2 *Faktorisati broj* $n = 89893$ *pomoću baza faktora ako je* $b = 20$.

Zadatak 13.3 *Faktorisati broj* $n = 17873$ *pomoću verižnih razlomaka ako je granica glatkosti* $b = 30$.

Zadatak 13.4 *Faktorisati broj* $n = 221$ *pomoću eliptičke krive* $E : y^2 = x^3 + x + 1$ *i tačke* $R = (0, 1)$ *na toj krivoj.*

Zadatak 13.5 *Napisati Python funkciju za faktorizaciju broja* $\boldsymbol{n}$ *primenom postupka Fermaove faktorizacije.*

14 Polje brojeva

Zadatak 14.1 *Pokazati da je* $f(x) = x^2 - 2$ *minimalni polinom polja koje je zatvoreno za operacije* $+, -, \times$ *i* $/$.

Zadatak 14.2 *Odrediti minimalni polinom broja* $\alpha = 2^{\frac{1}{3}} + 1$.

Zadatak 14.3 *Dokazati da su u polju* $\mathbb{Q}(\sqrt{-5})$ *svi algebarski celi brojevi oblika* $a + b\sqrt{-5}$, *gde su* a *i* b *celi brojevi.*

Zadatak 14.4 *Dokazati da se u polju* $Q(\sqrt{-5})$ *broj 2 ne može rastaviti u netrivijalni proizvod algebarskih celih brojeva.*

Zadatak 14.5 *Dokazati da 2 nije prost u* $Q(\sqrt{-5})$.

Zadatak 14.6 *Odrediti proste brojeve u* $\mathbb{Z}(i)$ *koji su manji od 30.*

Zadatak 14.7 *U skupu* $\mathbb{Z}(i)$ *rastaviti na činioce:*

a) $5 + 3i$

b) $11 - 3i$

c) $7 + i$

15 Vežba

Zadatak 15.1 *Odrediti sve generatore* $\mathbb{Z}/n\mathbb{Z}^*$ *za* $n = 11$.

Zadatak 15.2 *Odrediti* x *ako važi* $8^x \equiv 15 (mod\ 11)$

Zadatak 15.3 *Pomoću Euklidovog algoritma odrediti* $(x^3 + x^2)^{-1}$ *u polju* $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$.

Zadatak 15.4 *Šifrovati otvoreni tekst "kG " algoritmom SAES, ako je ključ "Ma".*

Zadatak 15.5 *Dešifrovati šifrat 1011 0000 0010 0101 algoritmom SAES, ako je ključ "Ma".*

Zadatak 15.6 *Prikazati postupak Massey-Omura razmene ključeva za* $q = 809$, $K = 97$, $e_A = 325$, $e_B = 517$.

Zadatak 15.7 *Prikazati razmenu poruka u sistemu RSA ako je* $n = 703$, $e = 611$, $M = 77$.

Zadatak 15.8 *Za eliptičku krivu* $E : y^2 = x^3 + x + 4$ *nad poljem* F_{11} *pokazati da je tačka* $(2, 5)$ *generator i napraviti tabelu umnožaka te tačke.*

Zadatak 15.9 *Eliptička kriva koja se koristi za problem usaglašavanja ključeva Diffie-Helman protokola je* $E : y^2 = x^3 + x + 4$ *nad poljem* $\mathbb{F}_{11}$*. Ako se koristi generator* $G = (9, 4)$*, tajni ključevi* $e_A = 5$*,* $e_B = 9$*, odrediti tačku koja se dobija kao rezultat usaglašavanja.*

Zadatak 15.10 *Za sistem El Gamal koristi se eliptička kriva* $E : y^2 = y^2 = x^3 + x + 4$ *nad poljem* $\mathbb{F}_{11}$*. Generator je* $G = (2, 6)$*. Ako su tajni ključevi* $e_A = 3$ *i* $e_B = 7$*, prikazati postupak šifrovanja poruke* $M = (9, 7)$ *(koristi se slučajan broj* $k = 5$*), a zatim postupak dešifrovanja šifrata.*

Zadatak 15.11 *Korisnik A ima javni ključ* $e = 11$*,* $n = 899$*. Kako glasi njegov RSA digitalni potpis poruke 876?*