Zadaća 1 iz Diskretne matematike

VAŽNA NAPOMENA: Pošto postavka zadaće zavisi od Vašeg broja indeksa, dužni ste ga napisati na naslovnoj stranici zadaće (to je onaj broj koji ste unijeli). Pri tome će se provjeravati da li je uneseni broj indeksa zaista Vaš! Također je neophodno jasno naznačiti grupu koju pohađate i odgovornog demonstratora za Vašu grupu.

Sve zadaće se predaju putem Zamgera u "`pdf`" formatu. Zadaće je moguće prethodno pripremiti putem nekog tekst procesora (poput MS Word-a) ili ih je moguće pisati rukom pa skenirati ili fotografirati. Uglavnom, prihvata se isključivo "`pdf`" format. Onim studentima koji budu zadaće uradili uz pomoć nekog tekst procesora opće namjene (poput MS Word-a) uz ispravno korištenje alata za pisanje matematičkih formula (tipa Equation editor ili nekog njemu sličnog) bodovi za zadaću biće uvećani za 15% u odnosu na bodove koje inače zaslužuju. S druge strane, studentima koji za izradu zadaće budu koristili LaTeX ili neki ekvivalentan visokoprofesionalni sistem za uređivanje matematičkih dokumenata, bodovi za zadaću biće uvećani za 30% u odnosu na bodove koje inače zaslužuju. Ti studenti moraju ponuditi dokaz da su zaista kreirali "`pdf`" dokument na taj način, tako što će umjesto samog "`pdf`" dokumenta poslati "`zip`" arhivu koja će sadržavati kako "`pdf`" dokument, tako i izvorni "`tex`" (ili neki analogni) dokument koji je iskorišten za kreiranje "`pdf`" dokumenta.

Krajnji rok za predaju zadaće je **ponedjeljak**, **6. XI 2017.** do kraja dana.

Unesite svoj broj indeksa (petocifreni): OK

Zadatak 1 [0.25 poena]

Za potrebe neke vitaminske terapije koriste se tri vrste tableta T_1, T_2 i T_3 koje respektivno sadrže 30, 33, odnosno 21 jedinica nekog vitamina. Terapijom je potrebno unijeti 210 jedinica tog vitamina. Odredite sve moguće načine kako se može realizirati ta terapija pomoću raspoloživih tableta ukoliko se tablete ne smiju lomiti, tj. može se uzeti samo cijela tableta.

Zadatak 2 [0.25 poena]

Čopor majmuna je skupljao banane. Kada su skupljene banane pokušali razmjestiti u 15 jednakih gomila, ispostavilo se da preostaje 9 banana koje je nemoguće rasporediti tako da gomile budu jednake. Slično, kada su probali rasporediti banane u 19 jednakih gomila, preostale su 2 banane. Međutim, uspjeli su skupljene banane razmjestiti u 28 jednakih gomila. Odredite koliki je najmanji mogući broj banana za koji je ovakav scenario moguć (uz pretpostavku da su majmuni u stanju uraditi ovo što je opisano, što je prilično diskutabilno).

Zadatak 3 [0.25 poena]

Tajna špijunska organizacija HABER SPY, zadužena za prisluškivanje razgovora na ETF Haber kutiji u cilju sprečavanja dogovaranja jezivih terorističkih aktivnosti koje se sastoje u podvaljivanju pokvarene (ukisle) kafe neposlušnim djelatnicima ETF-a, jednog dana uhvatila je tajanstvenu poruku koja je glasila

OECGJMZMXGHERZEXUOVZEHERVSDYEOEHNEXEHERJSXUOYZMDRMCEDMCEDUYM

Ova poruka smjesta je analizirana uz pomoć HEPEK superkvantnog kompjutera, koji nije uspio dešifrirati poruku, ali je došao do sljedećih spoznaja:

- Izvorna poruka je u cijelosti pisana bosanskim jezikom, isključivo velikim slovima unutar engleskog alfabeta (ASCII kodovi u opsegu od 65 do 91);
- Za šifriranje je korišten algoritam prema kojem se svaki znak izvorne poruke čiji je ASCII kod x mijenja znakom sa ASCII kodom y prema formuli $y = \mathrm{mod}(a\,x + b, 26) + 65$, gdje su a i b neke cjelobrojne konstante u opsegu od 0 do 25.

Međutim, HEPEK nije uspio do kraja probiti algoritam šifriranja i dešifrirati poruku. Stoga je vaš zadatak sljedeći:

a. Odredite konstante a i b ukoliko je poznata činjenica da se u bosanskom jeziku ubjedljivo najviše puta pojavljuje slovo A, a odmah zatim po učestanosti pojavljivanja slijedi slovo E;
b. Odredite funkciju dešifriranja, tj. funkciju kojom se vrši rekonstrukcija x iz poznatog y;
c. Na osnovu rezultata pod b), dešifrirajte uhvaćenu poruku (za tu svrhu, napišite kratku funkciju od dva reda u C-u, C++-u ili nekom drugom sličnom programskom jeziku, jer bi Vam ručno računanje oduzelo cijeli dan; uz zadaću, priložite listing te funkcije).

Zadatak 4 [0.6 poena]

Riješite sljedeće sisteme linearnih kongruencija i izdvojite im tipična rješenja:

a. $18\,x + 4\,y + 11\,z \equiv 62 \pmod{87}$, $2\,x + 18\,y + 15\,z \equiv 13 \pmod{87}$, $10\,x + 12\,y + 12\,z \equiv 59 \pmod{87}$
b. $15\,x + 3\,y \equiv 15 \pmod{102}$, $2\,x + 16\,y \equiv 6 \pmod{102}$

NAPOMENA: Čuvajte se neregularnih transformacija!

Zadatak 5 [0.8 poena]

Ispitajte rješivost i odredite broj rješenja sljedećih kvadratnih kongruencija (u slučaju da su rješive):

a. $x^2 \equiv 141 \pmod{1045}$
b. $x^2 \equiv 7801 \pmod{31096}$
c. $x^2 \equiv 20003 \pmod{4784}$
d. $x^2 \equiv 126 \pmod{38115}$

Zadatak 6 [1.2 poena]

Nađite sve diskretne kvadratne korijene sljedećih klasa ostataka, formiranjem odgovarajućih kvadratnih kongruencija i njihovim rješavanjem (rješavanje "grubom silom" neće biti prihvaćeno):

a. $[9]_{137}$
b. $[121]_{169}$
c. $[124]_{253}$
d. $[7506]_{9207}$

NAPOMENA: Nađena rješenja možete lako provjeriti modularnim kvadriranjem.

Zadatak 7 [0.25 poena]

Almira i Božidar žele da razmjenjuju poruke šifrirane nekim algoritmom koji zahtijeva tajni ključ, ali nemaju sigurnog kurira preko kojeg bi mogli prenijeti ključ. Zbog toga su odlučili da razmijene ključ putem Diffie-Hellmanovog protokola. Za tu svrhu, oni su se preko ETF Haber kutije dogovorili da će koristiti prost broj $p = 1013$ i generator $g = 5$. Nakon toga, Almira je u tajnosti slučajno izabrala broj $a = 329$, dok se Božidar u tajnosti odlučio za broj $b = 135$. Odredite koje još informacije Almira i Božidar moraju razmijeniti preko ETF Haber kutije da bi se dogovorili o vrijednosti ključa, te kako glasi ključ koji su oni dogovorili.

Zadatak 8 [0.4 poena]

Anita i Berin međusobno razmjenjuju poruke preko Facebook-a. Kako je poznato da takva komunikacija nije pouzdana, oni su odlučili da će primati samo šifrirane poruke. Anita je na svoj profil postavila informaciju da prima samo poruke šifrirane pomoću RSA kriptosistema s javnim ključem (599, 893), dok je Berin postavio informaciju da prima samo poruke šifrirane RSA kriptosistemom s javnim ključem (451, 1763).

a. Odredite kako glase tajni ključevi koje koriste Anita i Berin za dešifriranje šifriranih poruka koje im pristižu.
b. Odredite kako glase funkcije šifriranja i dešifriranja koje koriste Anita i Berin za šifriranje poruka koje šalju jedno drugom, odnosno za dešifriranje šifriranih poruka koje im pristižu.
c. Odredite kako glasi šifrirana poruka y koju Anita šalje Berinu ako izvorna poruka glasi $x = 6991$. Kako glasi digitalni potpis z u slučaju da Anita želi Berinu dokazati da poruka potiče baš od nje?
d. Pokažite kako će Berin dešifrirati šifriranu poruku y koju mu je Anita poslala (tj. primijenite odgovarajuću funkciju za dešifriranje na šifriranu poruku) i na osnovu primljenog digitalnog potpisa z utvrditi da je poruka zaista stigla od Anite.

NAPOMENA: Obratite pažnju da je poruka veća od modula enkripcije!