Zadaća 1

iz predmeta Diskretna Matematika

Prezime i ime: Mašović Haris

Br. indexa: 17993

Grupa: RI-4

Demonstrator: Rijad Muminović

Zadatak	Bodovi
1	
2	
3	
4	
5	
6	
7	
8	

Elektrotehnički fakultet Sarajevo - Oktobar 2017g.

1. Rješenje zadatka

Zadatak 1 [0.25 poena]

Za potrebe neke vitaminske terapije koriste se tri vrste tableta T1, T2 i T3 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.

* Ukoliko broj traženih tableta T1, T2 i T3 označimo respektivno sa x, y i z, problem se može formulisati u obliku diofantove jednačine i to na sljedeći način:

$$30x + 33y + 21z = 210$$

uz dodatne uslove x,y,z ∈ Z , x ≥ 0; y ≥ 0 i z ≥ 0.

Kako je NZD(30, 33, 21) = 3 i 3 | 210, jednačina je rješiva. Sada jednačinu možemo podijeliti sa 3 i dobiti njoj ekvivaletnu jednačinu

$$10x + 11y + 7z = 70$$

Napišimo ovu jednačinu u obliku $10x + 11y = 70 - 7z$. Kako je NZD(10, 11) = 1 rješenja će postojati ako i samo ako 1 | 70 - 7z, odnosno ako postoji k ∈ Z takav da je 70 - 7z = k, što daje novu diofantovu jednačinu

$$k + 7z = 70$$

Ovo je diofantova jednačina sa dvije nepoznate u kojoj je NZD(1, 7) = 1 i pri tome je ispunjen uvjet 1 | 70, pa možemo pristupiti rješavanju diofantove jednačine. Koristeći Euklidov algoritam odmah možemo izraziti 1 preko 1 i 7, tj.

$$7 = 1 \cdot 7 + 1 \cdot 0$$

Opće rješenje za ovu jednačinu glasi z = 70 + t; t ∈ Z. Vratimo se sada u početnu jednačinu 10x + 11y = 70 - 7z i uvrštavanjem z dobijamo:

$$10x + 11y = -420 - 7t$$

Sada moramo izraziti NZD(10, 11) = 1 kao linearnu kombinaciju 10 i 11. Primjenimo prošireni Euklidov algoritam:

$$1 = -1 \cdot 10 + 1 \cdot 11$$

Odavde slijede opća rješenja početne jednačine data sa:

$$x = 420 + 7t + 11s; \quad y = -420 - 7t - 10s; \quad z = 70 + t; \quad (RJ)$$

Prema postavci zadatka imamo x ≥ 0 , y ≥ 0 i z ≥ 0, što nam daje ograničenja pomoću kojih ćemo dobiti konkretne vrijednosti t i s. Iz uslova z ≥ 0 imamo 70 + t ≥ 0 tj. t ≥ -70. Iskoristimo sada uslove x ≥0 i y ≥ 0. Iz uslova x ≥ 0 i y ≥ 0 dobijamo

$$420 + 7t + 11s \geq 0 \quad i \quad -420 - 7t - 10s \geq 0$$

i dobijamo rješenja:

$$s \geq \frac{-(420 + 7t)}{11} \quad (1) \quad i \quad s \leq \frac{-(420 + 7t)}{10} \quad (2)$$

Spajanjem uslova (1) i (2) dobijamo slijedeću nejednakost, iz koje možemo izraziti još jedan uslov za parametar t i to na sljedeći način:

$$\frac{-(420+7t)}{11} \leq s \leq \frac{-(420+7t)}{10} \quad (0)$$

Očigledno vrijedi da je:

$$\frac{-(420+7t)}{11} \leq \frac{-(420+7t)}{10}$$

i na osnovu toga imamo rješenje: t ≤ -60 što ako presječemo sa t ≥ -70 imamo 10 cijelobrojnih rješenja i to takvih da t ∈ [-70,-60].

Sada za svako t iz skupa pobrojanih vrijednosti moramo odrediti moguće vrijednosti parametra s uvrštavajući vrijednost t u jednačinu (0).
Pa imamo 5 rješenja naše početne diofantove jednačine i to:

1. Uvrštavanjem t = -70 u (0) dobijamo naše s = 7, i uvršatavanjem toga u (RJ) imamo:

$$x = 7 \quad y = 0 \quad z = 0$$

2. Uvrštavanjem t = -69 u (0) dobijamo naše s = 6, i uvršatavanjem toga u (RJ) imamo:

$$x = 3 \quad y = 3 \quad z = 1$$

3. Uvrštavanjem t = -66 u (0) dobijamo naše s = 4, i uvršatavanjem toga u (RJ) imamo:

$$x = 2 \quad y = 2 \quad z = 4$$

4. Uvrštavanjem t = -63 u (0) dobijamo naše s = 2, i uvršatavanjem toga u (RJ) imamo:

$$x = 1 \quad y = 1 \quad z = 7$$

5. Uvrštavanjem t = -62 u (0) dobijamo naše s = 1, i uvršatavanjem toga u (RJ) imamo:

$$x = 0 \quad y = 0 \quad z = 10$$

2. Rješenje zadatka

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 rasporedititi 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).

* Ovaj problem se može predstaviti kao sistem linearnih kongruencija i to na sljedeći način:

$$x \equiv 9 \ (mod\ 15) \quad x \equiv 2 \ (mod\ 19) \quad x \equiv 0 \ (mod\ 28)$$

Kako je NZD(15, 19, 28) = 1 možemo koristiti Kinesku teoremu o ostacima pri rješavanju ovog sistema.

Izračunajmo $\lambda_1 = (15 \cdot 19 \cdot 28)/15 = 532$, $\lambda_2 = (15 \cdot 19 \cdot 28)/19 = 420$ i
$\lambda_3 = (15 \cdot 19 \cdot 28)/28 = 285$.

Opće rješenje se može predstaviti u obliku
$x \equiv \lambda_1 \cdot x_1 + \lambda_2 \cdot x_2 + \lambda_3 \cdot x_3 \pmod{15 \cdot 19 \cdot 28}$ (RJ)
gdje su x-vi rješenja posebnih jednačina, odnosno:

$$7 \cdot x_1 \equiv 9 \ (mod\ 15)\ (1) \quad 2 \cdot x_2 \equiv 2 \ (mod\ 19)\ (2) \quad 5 \cdot x_3 \equiv 0 \ (mod\ 28)\ (3)$$

Rješenja respektivno kongruencija su:

$$x_1 = 12\ (1) \quad x_2 = 1\ (2) \quad x_3 = 0\ (3)$$

Pošto smo našli x_1 x_2 i x_3 uvrstimo to u (RJ) i imamo naše rješenje datog problema:

$$x \equiv (532 \cdot 12 + 420 \cdot 1 + 285 \cdot 0 = 6804)\ (mod\ 7980)\ tj. \quad x \equiv 6804\ (mod\ 7980)$$

Najmanji mogući broj banana je 6804.

3. Rješenje zadatka

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

1. Izvorna poruka je u cijelosti pisana bosanskim jezikom, isključivo velikim slovima unutar engleskog alfabeta (ASCII kodovi u opsegu od 65 do 91);

2. 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 = 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).

a)

* Prebrojavanjem možemo zaključiti da se najviše ponavlja slovo E, a zatim slovo M, pa možemo pretpostaviti da se prilikom šifriranja slovo A zamijenilo sa slovom E, a slovo E sa slovom M. Kako slova A, E, M imaju redom ASCII šifre 65, 69, 77 to znači da uz navedenu pretpostavku a i b moraju zadovoljavati slijedeći sistem jednačina:

$$mod(65a + b, 26) + 65 = 69 \quad i \quad mod(69a + b, 26) + 65 = 77$$

odnosno:

$$mod(65a + b, 26) = 4 \quad i \quad mod(69a + b, 26) = 12$$

što dalje se može zapisati kao:

$$65a + b \equiv 4 \ (mod\ 26) \quad i \quad 69a + b \equiv 12 \ (mod\ 26)$$

Riješimo ovaj sistem, tako što ćemo pomnožiti prvu jednačinu sa (-1) i dodati na drugu, pri čemu imamo:

$$4a \equiv 8 \ (mod\ 26)$$

Naša dobivena jednačina predstavlja običnu diofantovu jednačinu:

$$4a + 26k = 8 \ -> \quad 2a + 13k = 4$$

NZD(2, 13) = 1 pa primjenom proširenog Euklidovog algoritma odmah u prvom koraku dobijamo da možemo 1 izraziti kao:

$$1 = -6 \cdot 2 + 1 \cdot 13$$

Imamo opće rješenje a = -24 + 13t; t $\in$ Z. Iz uslova 0 $\leq$ a $\leq$ 25 dobijamo vrijednosti t na sljedeći način: 0 $\leq$ -24 + 13t $\leq$ 25 dobijamo skup vrijednosti da t $\in$ {2,3}. Uvrstimo li t = 2 i t = 3 u a = -24 + 13t dobijamo a = 2 i a = 15 respektivno. Sada kada smo našli moguće vrijednosti a, vrijednosti b ćemo dobiti uvrštavanjem u jednu od kongruencija početnog sistema.
Uvrštavanjem u 65a + b $\equiv$ 4 (mod 26) dobijamo dvije kongruencije po b:

$$130 + b \equiv 4 \ (mod\ 26) \ za\ a = 2 \quad i \quad 975 + b \equiv 4 \ (mod\ 26) \ za\ a = 15$$

odnosno:

$$b \equiv -126 \ (mod\ 26) \ za\ a = 2 \ (1) \quad i \quad b \equiv -971 \ (mod\ 26) \ za\ a = 15 \ (2)$$

Rješavanje (1) i (2) daje redom b = -126 + 26t; t $\in$ Z i b = -971 + 26s; s $\in$ Z što uz uslov 0 $\leq$ b $\leq$ 25 daje t = 5 i s = 38 respektivno, što daje b = 4 za a = 2 i b = 17 za a = 15. Dakle imamo dvije mogućnosti, a = 2 i b = 4 i a = 15 i b = 17. Međutim, pošto za slučaj a = 2 i b = 4 (prema postupku kodiranja/šifriranja) dobijamo uvijek neparne vrijednosti tj. y = mod(2a + 4, 26) + 65, pošto mod(2a + 4, 26) je uvijek paran broj i pošto se dodaje 65 imamo uvijek neparan broj. S tim naš šifrirani kod ima J karakter čija je ASCII vrijednost 74, a to je paran broj. Samim tim prvi slučaj moramo odbaciti. Samim tim slijedi da su rješenja pod a) a = 15 i b = 17.

b) Sada znamo da funkcija šifriranja tačno glasi y = mod(15x + 17, 26) + 65. Međutim, za dobijanje funkcije dešifriranja treba ovaj izraz riješiti po x, uz dodatni uvjet $65 \leq x < 91$. Uvedimo smjenu x = 65 + z, tako da dodatni uvjet postaje $0 \leq z < 26$. Pokažimo to na sljedeći način:

$$y - 65 = mod(15x + 17, 26) -> 15x \equiv y - 82 \ (mod\ 26)$$

Uvedimo gore spomenutu smjenu: x = 65 + z, i dobit ćemo sljedeće:

$$15 \cdot z \equiv y - 17 \ (mod\ 26)$$

NZD(15,26) = 1, samim tim možemo riješiti ovu diofantovu jednačinu, a ostatak možemo napisati kao:

$$1 = 7 \cdot 15 - 4 \cdot 26$$

Na osnovu toga možemo formirati naše rješenje z kao:

$$z = 7 \cdot (y - 17) + 26t, \ gdje\ t\ \in Z$$

Odnosno naše rješenje možemo napisati i na sljedeći način:

$$z \equiv 7y - 119 \ (mod\ 26) -> \ z \equiv 7y + 11 \ (mod\ 26)$$

Uvrštavanjem smjene za z imamo:

$$x = mod(7y + 11, 26) + 65$$

što ujedno predstavlja naš glavni dio dekodiranja zadane šifrirane poruke.

c)

Predstavimo ćemo našu formulu u c++ programu (tj. samo main je dovoljan):

```
int main() {

std::string a{"OECGJMZMXGHERZEXUOVZEHERVSDYEOEHNEXEH"
"ERJSXUOYZMDRMCEDMCEDUYM"};    // a je naša poruka
for (int i=0; i < a.length(); i++) a[i] = char(((7*a[i]+11) % 26) + 65);
std::cout « a;

}
```

** Kao rezultat dobijamo poruku:
SAMOJEREDOVANRADISPRAVANPUTKASAVLADAVANJUDISKRETNEMATEMATIKE
odnosno da odvojimo:
SAMO JE REDOVAN RAD ISPRAVAN PUT KA SAVLADAVANJU DISKRETNE MATEMATIKE

4. Rješenje zadatka

Zadatak 4 [0.6 poena]

a)

$$18x + 14y + 11z \equiv 62 \ (mod\ 87) \ (1)$$
$$2x + 18y + 15z \equiv 13 \ (mod\ 87) \ (2)$$
$$10x + 12y + 12z \equiv 59 \ (mod\ 87) \ (3)$$

Ukoliko (2) jednačinu pomnožimo sa (-9) i dodamo na (1), i ukoliko (2) jednačinu pomnožimo sa (-5) i dodamo na (3) imamo sljedeće:

$$158y + 124z \equiv 55 \ (mod\ 87)$$
$$78y + 63z \equiv 6 \ (mod\ 87)$$

Pomnožimo našu drugu jednačinu sa (-2) i saberimo sa prvom, pa na osnovu toga imamo:

$$158y + 124z \equiv 55 \ (mod\ 87)$$
$$2y - 2z \equiv 43 \ (mod\ 87)$$

Ukoliko sad pomnožimo našu drugu jednačinu sa 62 imamo (to smijemo uraditi jer je NZD(62,87 = 1):

$$158y + 124z \equiv 55 \ (mod\ 87)$$
$$124y - 124z \equiv 2666 \ (mod\ 87) -> \ 124y - 124z \equiv 56 \ (mod\ 87)$$

Saberimo sad ove 2 jednačine i izvršimo skraćenje po modulu:

$$21y \equiv 24 \ (mod\ 87)$$

Ovo predstavlja običnu diofantovu jednačinu koju možemo zapisati kao:

$$21y + 87k = 24, \ k \in Z$$

Pošto je NZD(21,87) = 3, podijelimo jednačin sa 3 i samim tim je ona rješiva:

$$7y + 29k = 8$$

Pošto je NZD(7,29) = 1, to možemo zapisati u obliku:

$$1 = -4 \cdot 7 + 1 \cdot 29$$

Na kraju imamo da je rješenje po y:

$$y = -32 + 29t, \ t \in Z$$

odnosno da bi dobili tipična rješenja uvrstimo t=2, t=3, t=4 respektivno:

$$y = 26 \quad y = 55 \quad y = 84$$

Pošto smo našli par kombinacija y, uvrstimo npr. prvo rješenje nazad u jednačinu 2y - 2z ≡ 43 (mod 87) pri čemu ćemo kao finalni izraz dobiti:

$$2z + 87k = 9, \ k \in Z$$

Ukoliko ponovimo postupak za rješavanje diofantove jednačine (uradili smo ga n-puta dosad) imamo da je rješenje:

$$z = -387 + 87t,\ t \in Z$$

odnosno da naša tipična rješenje za z su (ukoliko ponovimo uvrštavanje za svaki y) respektivno:

$$z = 48 \quad z = 77 \quad z = 19$$

Ukoliko sada uvrstimo bilo koju varijantu y i z u početnu (2) jednačinu, konkretno ovdje za prvo y i z, dobijamo novu diofantovu jednačinu:

$$2x + 87t = 43,\ t \in Z$$

Rješenje ove diofantove jednačine je:

$$x = -1849 + 87t$$

odnosno naše tipično rješenje:

$$x = 65$$

Pri čemu se može pokazati da i za ostale kombinacije y i z, dobije se x = 65. Možemo zaključiti da su rješenja našeg sistema linearnih kongruencija tj. tipična rješenja:

$$x = 65 \quad y = 26 \quad z = 48$$

$$x = 65 \quad y = 55 \quad z = 77$$

$$x = 65 \quad y = 84 \quad z = 19$$

b)

$$15x + 3y \equiv 15\ (mod\ 102)$$

$$2x + 16y \equiv 6\ (mod\ 102)$$

Ukoliko našu 2 jednačinu pomnožimo sa (-7) i dodamo na prvu imamo:

$$x - 109y \equiv -27\ (mod\ 102)$$

$$2x + 16y \equiv 6\ (mod\ 102)$$

Sada ako pomnožimo prvu sa (-2) i dodamo na drugu imamo sistem:

$$x - 109y \equiv -27\ (mod\ 102)\ (1)$$

$$30y \equiv 60\ (mod\ 102)\ (2)$$

Riješimo zasebno drugu jednačinu što predstavlja običnu diofantovu jednačinu. Pošto je NZD(30,102) = 6, ukoliko jednačinu podijelimo sa 6 imamo:

$$5y + 17k = 10,\ k \in Z$$

NZD(5, 17) = 1, preko proširenog Euklidovog algoritma imamo:

$$1 = 7 \cdot 5 - 2 \cdot 17$$

odnosno naše rješenje za y:

$$y = 70 + 17t,\ t \in Z$$

Da bismo dobili tipična rješenja za y, moramo ograničiti y i to tako da važi:

$$0 \leq 70 + 17t < 102$$

odnosno dobijamo skup t takav da t $\in$ {-4,-3,-2,-1,0,1}. Samim tim naša rješenja su respektivno za y:

$$y \in \{2, 19, 36, 53, 70, 87\}$$

Uvrštavanjem svakih od y-ona u (1) i rješavanjem zasebno diofantovih jednačina imamo da su rješenja respektivno (što smo već radili više puta do sad):

$$x \in \{89, 4, 21, 38, 55, 72\}$$

odnosno naš sistem ima 6 rješenja i to:

$$x = 89 \quad y = 2 \ (1)$$

$$x = 4 \quad y = 19 \ (2)$$

$$x = 21 \quad y = 36 \ (3)$$

$$x = 38 \quad y = 53 \ (4)$$

$$x = 55 \quad y = 70 \ (5)$$

$$x = 72 \quad y = 87 \ (6)$$

5. Rješenje zadatka

Zadatak 5 [0.8 poena]

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

a)

$$x^2 \equiv 141 \ (mod \ 1045)$$

Očigledno 1045 je složen broj, i može se raspisati kao $1045 = 2^0 \cdot 5 \cdot 11 \cdot 19$. Dalje pošto je NZD(141, 1045) = 1, mora važiti uslov da je da je kvadratni ostatak 141 po svakom modulu 5, 11, 19.
Odnosno mora važiti p(141 | 5) i p(141 | 11) i p(141 | 19).
Prvi uslov važi pošto je mod(141,5) = 1, pa imamo p(1 | 5) = 1.
Iz drugog uslova važi mod(141,11) = 9, pa imamo $p(3^2 \mid 11) = 1$.
Iz trećeg uslova važi mod(141,19) = 8, pa imamo $p(2^3 \mid 19) = p(2^2 \mid 19)\ p(2 \mid 19) =$
$= p(2 \mid 19) = (-1)^{(19^2-1)/8}$ = -1

Naša kvadratna kongruencija očigledno nije rješiva.

b)

$$x^2 \equiv 7801 \ (mod \ 31096)$$

Očigledno 31096 je složen broj, i može se raspisati kao $31096 = 2^3 \cdot 13^2 \cdot 23$. Dalje pošto je NZD(7801, 31096) = 1, mora važiti uslov da je da je kvadratni ostatak 7801 po svakom od modula 13, 23.

Odnosno mora važiti p(7801 | 13) i p(7801 | 23) i nameće se dodatni uslov da je
$7801 \equiv 1 \pmod 8$ koji je bezuvjetno tačan.
Prvi uslov važi pošto je mod(7801,13) = 1, pa imamo p(1 | 13) = 1.
Iz drugog uslova važi mod(7801, 23) = 4, pa imamo $p(2^2 \mid 23) = 1$.
Odnosno pošto je kvadratna kongruencija rješiva, broj tipičnih rješenja kongruencije je 2^{k+2}, odnosno 16.

c)

$$x^2 \equiv 20003 \ (mod\ 4784)$$

Očigledno 4784 je složen broj, i može se raspisati kao $31096 = 2^4 \cdot 13 \cdot 23$. Dalje pošto je NZD(20003, 4784) = 1, mora važiti uslov da je da je kvadratni ostatak 20003 po svakom od modula 13, 23. Odnosno mora važiti p(20003 | 13) i p(20003 | 23) i nameće se dodatni uslov da je $20003 \equiv 1 \pmod 8$ koji nije tačan, jer je ostatak 3, samim tim naša kvadratna kongruencija nije rješiva.

d)

$$x^2 \equiv 126 \ (mod\ 38115)$$

Očigledno je NZD(126, 38115) = 63, samim tim mora se transformisati početni izraz tako da bude ovaj potreban uslov zadovoljen. Broj 63 možemo izraziti kao:

$$63 = 7 \cdot 3^2$$

gdje p=7 a q=3^2, što povlači narednu diofantovu jednačinu:

$$7z \equiv 2 \ (mod\ 605)$$

NZD(2,605) = 1, i može se izaziti kao:

$$1 = 173 \cdot 7 - 2 \cdot 605$$

i naše tipično rješenje je $z_0 = 346$.
Na osnovu toga dobivamo novu oformljenu kvadratnu kongruenciju:

$$y^2 \equiv 346 \ (mod\ 605)$$

Očigledno 605 je složen broj, i može se raspisati kao $605 = 2^0 \cdot 5 \cdot 11^2$. Dalje pošto je NZD(346, 605) = 1, mora važiti uslov da je da je kvadratni ostatak 346 po svakom modulu 5, 11.
Odnosno mora važiti p(346 | 5) i p(346 | 11).
Prvi uslov važi pošto je mod(346,5) = 1, pa imamo p(1 | 5) = 1.
Drugi uslov važi pošto je mod(346,11) = 5, pa imamo p(5 | 11) = p(1 | 11) = 1.
Očigledno je nova kvadratna kongruencija rješiva, i broj tipičnih rješenja kvadratne kongruencije je 2^k, odnosno $2^2 = 4$. Da bismo dobili ukupan broj tipičnih rješenja početne kvadratne kongruencije, moramo ovaj broj pomnožiti sa q, odnosno naš finalni broj tipičnih kongruentnih rješenja je $4 \cdot 3 = 12$.

6. Rješenje zadatka

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. $[7506]_{9207}$

a) $[9]_{137}$
Ovo možemo napisati u obliku kvadratne kongruencije:

$$x^2 \equiv 9 \ (mod\ 137)$$

Pošto je NZD(9, 137) = 1 i (9 | 137) = 1 kongruencija je rješiva i ona ima dva tipična rješenja. Ukoliko je x_1 jedno tipično rješenje ove kongruencije, onda je p - x_1 drugo tipično rješenje. Pošto mod(137, 4) = 1 i mod(137, 8) = 1 rješenje tražimo pomoću Tonellijevog algoritma. Da bi koristili Tonellijev algoritam moramo naći broj g takav da je (g | 137) = -1. Pokušajmo sa g=3: $(3 \mid 137) = (137 \mid 3) \cdot (-1)^{(136 \cdot 2)/4} = (2 \mid 3) = -1$

Sada su početni parametri za Tonellijev algoritam t = 68 , v = 1, w = 9, h = $([3]_{137})^{-1}$.
Parametar h možemo izračunati kao rješenje kongruencije:

$$3x \equiv 1 \ (mod\ 137)$$

odnosno naš h = 46 kad se riješi ova diofantova jednačina.
Predstaviti ćemo naš Tonellijev algoritam pomoću c++ kod-a koji će kao rezultat dati x i p - x:

```
int p = 137, g=3;
int t= 68, v = 1, w = 9, h = 46;
int x;
while(t % 2 == 0){
t = t/2; h = ((h*h) % p);
if((int(std::pow(w,t)) % p) != 1){
v = (v * g) % p;
w = (w * h) % p;
}
g = int(std::pow(w,2)) % p;
}
x = (v * int(std::pow(w, (t+1)/2))) % p;

std::cout « x « " " « p - x;
```

Kao rezultat dobijamo $x_1 = 3$ i $x_2 = 134$. Ovo su ujedno i svi diskretni kvadratni korijeni zadane početne kvadratne kongruencije.

b) $[121]_{169}$

Ovo možemo napisati u obliku kvadratne kongruencije:

$$x^2 \equiv 121 \ (mod\ 169)$$

Ispitajmo uslove rješivosti. 169 se može napisat kao 13^2 samim tim je složen broj, a NZD(121,169) = 1, samim tim slijedi da (121 | 169) = 1. Očigledno su svi uslovi zadovoljeni i naša kvadratna kongruencija je rješiva. Broj naših tipičnih rješenja je $2^1 = 2$.
Pređimo na rješavanje:
Naša rješenja zadane kvadratne kongruencije se svedu na rješavanje kongruencije:

$$x^2 \equiv 121 \ (mod\ 13)$$

Pošto je 13 prost broj i NZD(121, 13) = 1 i (121 | 13) = 1 naša kvadratna kongruencija je rješiva. Pošto je 13 prost broj, vidimo da važi Legendrov uslov mod(13,8) = 5. Prema Legendrovoj formuli imamo da je x = mod($121^{(13+3)/8}$, 13) = 3. Ispitajmo mod(x^2, 13) = 121, očigledno je različito, i x ne zadovoljava kongruenciju. Ukoliko primjenimo drugu Legendrovu formulu imamo rješenje $x_1 = 11$ odnosno $x_2 = 2$.

Odnosno nazovimo $x_1 = 2$ sad.
Izračunajmo $[h]_p = ([2x_1]_p)^{-1}$. Ovo se svodi na rješavanje kongruencije 4x ≡ 1 (mod 13) čije je tipično rješenje x = 10, pa je h = 10.
Sada x_2 računamo kao x_2 = mod(x_1 - h ·((x_1)^2 - a), 13^2) = 158.
Odnosno naša dva finalna rješenja su: $x_1 = 11$ (169 - 158) i $x_2 = 158$.

c) $[124]_{253}$

Ovo možemo napisati u obliku kvadratne kongruencije:

$$x^2 \equiv 124 \ (mod\ 253)$$

NZD(124, 253) = 1, ali 253 se može napisati kao $253 = 2^0 \cdot 11 \cdot 23$. (124 | 253) = 1, samim tim broj rješenja zadane kvadratne kogruencije je $2^2 = 4$. Moramo ispitati riješivost i rješiti naredne dvije kongruencije:

$$x^2 \equiv 124 \ (mod\ 11) \ -> \ x^2 \equiv 3 \ (mod\ 11)$$

$$x^2 \equiv 124 \ (mod\ 23) \ -> \ x^2 \equiv 9 \ (mod\ 23)$$

Prva kongruencija je rješiva jer je (3 | 11) = 1, samim tim i druga jer je (3^2 | 23) = 1. Nije teško vidjeti na prvu da su rješenja prve kongruencije $x_1 = 5$ i $x_2 = 6$ (mada možemo primjeniti i neki metod na osnovu prethodnih zadataka) i rješenja druge kongruencije $x_3 = 3$ i $x_4 = 20$. Formirajmo kombinacije tipičnih rješenja kao: (5,3),(5,20),(6,3),(6,20). Odnosno naravno sada rješavamo preko kineske teoreme o ostacima (primjer: zadatak 2) ili običnim putem uvrštavanja i pri čemu dobijamo respektivno 4 sistema linearnih kongruencija iz kojih slijedi 4 rješenja početne kvadratne kongruencije:

1. za (5,20) –> $x_1 = 181$,
2. za (5,3) –> $x_2 = 49$,
3. za (6,3) –> $x_3 = 72$,
4. za (6,20) –> $x_4 = 204$.

d) $[7506]_{9207}$

Ovo možemo napisati u obliku kvadratne kongruencije:

$$x^2 \equiv 7506 \ (mod\ 9207)$$

NZD(7506, 9207) = 27, pa moramo transformisati našu kvadratnu kongruenciju. Odnosno naš $27 = 3^3 = 3{\cdot}3^2$. Formiramo linearnu kongruenciju:

$$3z \equiv 278 \ (mod\ 341)$$

Pri čemu rješenje ove linearne kongruencije je $z_0 = 320$. Sad moramo ispitati rješivost kvadratne kongruencije:

$$x^2 \equiv 320 \ (mod\ 341)$$

NZD(320,341) = 1, a modul $341 = 11 \cdot 31$. Također važi $(320 \mid 11) = 1$ i $(320 \mid 31) = 1$. Samim ti je naša kvadratna kongruencija rješiva i ima $2^2 = 4$ rješenja. Odnosno naša početna kvadratna kongruencija je rješiva i ima $4 \cdot 3 = 12$ rješenja. Riješimo sada našu novu kvadratnu kongruenciju:

$$x^2 \equiv 320 \ (mod\ 341)$$

odnosno moraju biti rješive naredne kongruencije:

$$x^2 \equiv 320 \ (mod\ 11) \ -> \ x^2 \equiv 1 \ (mod\ 11)$$

$$x^2 \equiv 320 \ (mod\ 31) \ -> \ x^2 \equiv 10 \ (mod\ 31)$$

Rješenja ovih kvadratnih kongruencija (moduli su prosti pa se računanje ove dvije kvaratne kongruencije svede na računanje sistema preko kineske teoreme tj. računanje 4 sistema specifična za 4 tipična rješenja ovih kvadratnih kongruencija):

$$x_1 = 45 \quad x_2 = 76 \quad x_3 = 265 \quad x_4 = 296$$

Odnosno da bismo dobili naših 12 rješenja, svakom ovom tipičnom rješenju odgovaraju još 3 tipična rješenja za prvu kvadratnu kongruenciju prema formuli

$$9 \cdot x + 3096 \cdot i, \ gdje\ i \ = \ 0, 1, 2$$

odnosno

$$x_1 = 405 \quad x_2 = 3474 \quad x_3 = 6543 \quad za\ x = 45$$

$$x_4 = 684 \quad x_5 = 3753 \quad x_6 = 6822 \quad za\ x = 76$$

$$x_7 = 2385 \quad x_8 = 5454 \quad x_9 = 8523 \quad za\ x = 265$$

$$x_{10} = 2664 \quad x_{11} = 5733 \quad x_{12} = 8802 \quad za\ x = 296$$

7. Rješenje zadatka

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.

* Almira i Božidar su se dogovorili da koriste prost broj p = 1013 i generator g = 5. Pošto je Almira izabrala u tajnosti broj a = 329 ona računa $\alpha = \text{mod}(g^a, \text{p}) = \text{mod}(5^{329}, 1013) = = [5]^{329}_{1013}$. Božidar je izabrao broj b = 135 pa računa $\beta = \text{mod}(g^b, \text{p}) = \text{mod}(5^{135}, 1013) = = [5]^{135}_{1013}$. Za izračunavanje potrebnih modula, koristiti ćemo metodu kvadriraj-i-množi. Raspišimo prvo eksponente koji su nam potrebni pomoću stepena dvojke:
$329 = 256 + 64 + 8 + 1$,
$135 = 128 + 4 + 2 + 1$.

Sada računamo sve stepene:

$$\begin{aligned}
[5]^2_{1013} &= [25]_{1013} \\
[5]^4_{1013} &= [625]_{1013} \\
[5]^8_{1013} &= [620]_{1013} \\
[5]^{16}_{1013} &= [473]_{1013} \\
[5]^{32}_{1013} &= [869]_{1013} \\
[5]^{64}_{1013} &= [476]_{1013} \\
[5]^{128}_{1013} &= [677]_{1013} \\
[5]^{256}_{1013} &= [453]_{1013}
\end{aligned}$$

Sada imamo da je:

$$[5]^{329}_{1013} = [453]_{1013} \cdot [476]_{1013} \cdot [620]_{1013} \cdot [5]_{1013}$$
$$[5]^{329}_{1013} = [516]_{1013}$$

odnosno:

$$[5]^{135}_{1013} = [677]_{1013} \cdot [625]_{1013} \cdot [25]_{1013} \cdot [5]_{1013}$$
$$[5]^{135}_{1013} = [882]_{1013}$$

Dakle, Almira je izračunala $\alpha = 516$ i šalje to Božidaru, a Božidar je izračunao $\beta = 882$ i šalje to Almiri. Sada i Almira i Božidar u tajnosti računaju vrijednost ključa. Almira računa po formuli $\text{k} = \text{mod}(\beta^a, \text{p})$ dok Božidar ključ računa po formuli $\text{k} = \text{mod}(\alpha^b, \text{p})$.

Almira računa:

$$k = mod(\beta^a, p) = mod(882^{329}, 1013) = [882]^{329}_{1013}$$

$$\begin{aligned}
[882]^{2}_{1013} &= [953]_{1013} \\
[882]^{4}_{1013} &= [561]_{1013} \\
[882]^{8}_{1013} &= [691]_{1013} \\
[882]^{16}_{1013} &= [358]_{1013} \\
[882]^{32}_{1013} &= [526]_{1013} \\
[882]^{64}_{1013} &= [127]_{1013} \\
[882]^{128}_{1013} &= [934]_{1013} \\
[882]^{256}_{1013} &= [163]_{1013}
\end{aligned}$$

odnosno:

$$k = [882]^{329}_{1013} = [163]_{1013} \cdot [127]_{1013} \cdot [691]_{1013} \cdot [882]_{1013} = 543$$

Božidar računa:

$$k = mod(\alpha^b, p) = mod(516^{135}, 1013) = [516]^{135}_{1013}$$

$$\begin{aligned}
[516]^{2}_{1013} &= [850]_{1013} \\
[516]^{4}_{1013} &= [231]_{1013} \\
[516]^{8}_{1013} &= [685]_{1013} \\
[516]^{16}_{1013} &= [206]_{1013} \\
[516]^{32}_{1013} &= [903]_{1013} \\
[516]^{64}_{1013} &= [957]_{1013} \\
[516]^{128}_{1013} &= [97]_{1013} \\
[516]^{256}_{1013} &= [292]_{1013}
\end{aligned}$$

odnosno:

$$k = [516]^{135}_{1013} = [97]_{1013} \cdot [231]_{1013} \cdot [850]_{1013} \cdot [516]_{1013} = 543$$

Vidimo da su i Almira i Božidar došli do istog ključa, što znači da su razmijenili sve potrebne (i korektne) informacije.

8. Rješenje zadatka

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: Svo kvadriranje modula je već urađeno u primjerima iznad, tako da sam skratio ovdje da ne bi ispalo glomazno. Temelji se na istom načinu kao u prethodnom zadatku.. **
a) i b)

* Kako je Anita odredila da može primati šifrirane poruke ključem (599, 893), to znači da će prema RSA protokolu, Berin moći koristiti encoding funkciju koja glasi:

$$E_B(x) = mod(x^{599}, 893).$$

Analogno, kako Berin prima poruke šifrirane ključem (451, 1763) to znači da će Anita moći koristiti encoding funkciju koja glasi:

$$E_A(x) = mod(x^{451}, 1763).$$

Da bi se desila intercepcija, to zahtjeva proračunavanje ključeva tj. provaljivanje RSA protokola. Računamo sad tajne ključeve zasebno:

$$451 \cdot b_B \equiv 1 \ (mod \ \varphi(1763)) \ -> \ 1763 = 43 \cdot 41$$

$$451 \cdot b_B \equiv 1 \ (mod \ 1680)$$

$$b_B = 1531$$

Odnosno tajni ključ za Anitu:

$$599 \cdot b_A \equiv 1 \ (mod \ \varphi(893)) \ -> \ \ 893 = 19 \cdot 47$$

$$599 \cdot b_A \equiv 1 \ (mod \ 828)$$

$$b_A = 47$$

Odnosno imamo respektivno decoding formule:

$$D_B(y) = mod(y^{1531}, 1763)$$

$$D_A(y) = mod(y^{47}, 893)$$

c)

Neka je sada poruka koju Anita želi poslati Berinu x = 6991. Pošto je ova poruka veća no enkripcijski modul, mora se "razbiti" na dijelove. Odnosno:

$$6991_{10} = (3 \cdot 1702)_{1763}$$

Odnosno Anita šalje sljedeće enkripcije:

$$y_1 = mod(3^{451}, 1763) = 1667$$

$$y_0 = mod(1702^{451}, 1763) = 963$$

Koeficijente y_0 i y_1 Anita će poslati Berinu zajedno sa potpisom z. Taj potpis će Anita izračunati kao Berinovu enkripciju svoje dekripcije poruke koju mu želi poslati. Dakle,

$$z = E_B(D_A(6991))$$

Međutim, kako je 6991 veće od Anitinog dekripcionog modula, moramo "razbiti" i to na dijelove, odnosno:

$$6991_{10} = (7 \cdot 740)_{893}$$

odnosno:

$$D_A(6991) = D_A(7) \cdot 893 + D_A(740) \ -> \ \ D_A(7) = 524 \quad D_A(740) = 740$$

Odnosno z će se poslati u porukama i to:

$$z_1 = mod(524^{599}, 893) = 7$$

$$z_0 = mod(740^{599}, 893) = 740$$

d)

Sad Berin primjenjuje svoju dekripciju na y_1 i y_0:

$$D_B(1677) = mod(1677^{1531}, 1763) = 3$$

$$D_B(963) = mod(963^{1531}, 1763) = 1702$$

I računa poruku:

$$x = 3 \cdot 1763 + 1702 = 6991$$

Također ukoliko apsolutno želi biti siguran da je poruka od Anite, primjeniti će Anitinu enkripciju na svoju dekripciju pojedinačnih z_1 i z_0 odnosno:

$$D_B(z_1) = D_B(7) = 1221 -> E_A(1221) = 7 \quad (1)$$

$$D_B(z_2) = D_B(740) = 490 -> E_A(490) = 740 \quad (2)$$

odnosno kad sklopimo sve zajedno imamo:

$$x = (1) \cdot 893 + (2) = 6991$$

čime je upravo dokazana valjanost digitalnog potpisa, odnosno Anita je zaista poslala poruku Berinu.