

# Diskretna matematika

## Zadaća 1

Vedad Fejzagić

2017

## Zadatak 1

Ako označimo tablete T1, T2 i T3 kao  $x$ ,  $y$  i  $z$  respektivno, problem svodimo na rješavanje sljedeće diofantove jednačine sa 3 nepoznate:

$$15x + 33y + 27z = 162$$

Očigledno je da vrijedi:

$$NZD(15, 33, 27) = 3$$

Dokažimo koristeći Euklidov algoritam:

$$\begin{aligned} NZD(15, 33, 27) &= NZD(NZD(15, 33), 27) = \\ &= NZD(3, 27) = NZD(27, 3) = 3 \end{aligned}$$

Dalje, s obzirom da je  $NZD(15, 33, 27) = 3, 3 \mid 162$ , zadana diofantova jednačina je rješiva. Podijelimo je sa 3 i prebacimo  $z$  na desnu stranu:

$$15x + 33y + 27z = 162$$

$$5x + 11y + 9z = 54$$

$$5x + 11y = 54 - 9z$$

Pošto je  $NZD(5, 11) = 1$ , rješenja za  $x$  i  $y$  će postojati akko je  $1 \mid (54 - 9z)$  tj. ako postoji  $k \in \mathbb{Z}$  takav da vrijedi  $54 - 9z = k$  tj.  $k + 9z = 54$ . Ovo je diofantova jednačina, dakle  $NZD(9, 1) = 1, 1 \mid 54$ , te je potrebno izraziti  $NZD(9, 1) = 1$  kao linearnu kombinaciju 9 i 1:

$$9 = 1 \cdot 8 + 1 \implies 1 = 9 - 1 \cdot 8$$

Jedno rješenje je:

$$\begin{aligned}z^* &= 54 \\k^* &= -8 \cdot 54 = -432\end{aligned}$$

Opće rješenje za  $z(k$  nas ne interesuje za konkretan problem):

$$z = 54 + t, t \in \mathbb{Z}$$

Vraćamo u početnu jednačinu:

$$\begin{aligned}5x + 11y &= 54 - 9(54 + t) \\5x + 11y &= -432 - 9t\end{aligned}$$

Dobivena jednačina je diofantova. Očigledno je  $NZD(5, 11) = 1$ , potrebno je izraziti  $NZD(5, 11) = 1$  preko linearne kombinacije 5 i 11:

$$11 = 2 \cdot 5 + 1 \implies 1 = 11 - 2 \cdot 5 = -2 \cdot 5 + 11$$

Pa su opća rješenja:

$$\begin{aligned}x &= 864 + 18t + 11s \\y &= -432 - 9t - 5s \\z &= 54 + t \\t, s &\in \mathbb{Z}\end{aligned}$$

uz ograničenja  $x, y, z > 0$

Pristupamo rješavanju sistema nejednačina:

$$x = 864 + 18t + 11s > 0 \quad (1)$$

$$y = -432 - 9t - 5s \implies y = 432 + 9t - 5s < 0 \quad (2)$$

$$z = 54 + t > 0 \implies t > -54$$

Iz (2):

$$s < \frac{-9t - 432}{5} \quad (A)$$

Iz (1):

$$s > \frac{-864 - 18t}{11} \quad (B)$$

Možemo zaključiti:

$$\begin{aligned} (1) \wedge (2) &\implies \frac{-9t - 432}{5} > s > \frac{-864 - 18t}{11} \\ (-9t - 432) \cdot 11 &> (-864 - 18t) \cdot 5 \\ -9t - 432 &> 0 \\ t &< \frac{-432}{9} \\ t &< -48 \end{aligned}$$

Rješenja za t:

$$(t > -54) \wedge (t < -48) \implies t \in (-48, -54)$$

tj.

$$t \in [-49, -53], t \in \mathbb{Z}$$

Dalje, računamo vrijednost  $s$ ,  $\forall t \in [-49, -53] \wedge t \in \mathbb{Z}$  koristeći nejednakosti A i B. Lahko se pokaže da vrijednosti  $t = -49$ ,  $t = -50$  i  $t = -53$  ne daju vrijednost  $s \in \mathbb{Z}$ , dakle te vrijednosti odbacujemo.

Za  $t = -51$ :

$$(A) \implies s < \frac{27}{5} (= 5.4)$$

$$(B) \implies s > \frac{54}{11} (\sim 4.9)$$

$$s \in \left( \frac{54}{11}, \frac{27}{5} \right)$$

Pa jedina vrijednost u skupu  $Z$  na dobivenom intervalu je  $s = 5$ . Tu vrijednost i uzimamo.

Za  $t = -52$ :

Na sličan način kao i na prethodnom primjeru dobijamo vrijednost  $s = 7$ .

Zaključujemo da postoje dva rješenja, te ih uvrštavamo u opšta:

Za  $t = -51 \wedge s = 5$

$$x = 1, y = 2, z = 3$$

$$Provjera : 1 \cdot 15 + 2 \cdot 33 + 3 \cdot 27 = 162$$

Za  $t = -52 \wedge s = 7$

$$x = 5, y = 1, z = 2$$

$$Provjera : 5 \cdot 15 + 1 \cdot 33 + 2 \cdot 27 = 162$$

Dakle, postoje dva načina realizacije terapije; prvi način je jedna tableta T1, dvije tablete T2 i tri tablete T3; drugi način je pet tableta T1, jedna tableta T2 i dvije tablete T3.

## Zadatak 2

Zadani problem možemo predstaviti u obliku sistema linearnih kongruencija, gdje je  $x$  traženi minimalni broj banana:

$$\begin{aligned}x &\equiv 8 \pmod{9} \rightarrow NZD(1, 9) = 1 \\x &\equiv 2 \pmod{10} \rightarrow NZD(1, 10) = 1 \\x &\equiv 0 \pmod{17} \rightarrow NZD(1, 17) = 1\end{aligned}$$

Dakle, sistem linearnih kongruencija je rješiv što slijedi upravo iz rješivosti svih kongruencija pojedinačno. Rješavamo koristeći kinesku teoremu o ostacima. Najprije provjeramo da li je možemo primjeniti:

$$\begin{aligned}NZD(9, 10) &= 1 \\NZD(9, 17) &= 1 \\NZD(10, 17) &= 1\end{aligned}$$

Očigledno je da kinesku teoremu o ostacima možemo primjeniti.

$$n_1 \cdot n_2 \cdot n_3 = 9 \cdot 10 \cdot 17 = 1530$$

$$\lambda_1 = \frac{1530}{9} = 170$$

$$\lambda_2 = \frac{1530}{10} = 153$$

$$\lambda_3 = \frac{1530}{17} = 90$$

Rješenje možemo predstaviti u obliku:

$$x = 170x_1 + 153x_2 + 90x_3 \pmod{1530}$$

Pri čemu su  $x_1, x_2, x_3$  ma koja rješenja sistema linearnih kongruencija:

$$170x_1 \equiv 8 \pmod{9} \quad (A)$$

$$153x_2 \equiv 2 \pmod{10} \quad (B)$$

$$90x_3 \equiv 0 \pmod{17}$$

$x_3$  je očigledno bilo koji cijeli broj, dakle  $x_3 = 0$

Kongruencije (A) i (B) možemo jednostavno skratiti, te ih izraziti kao diofantove jednačine pa naći potrebnu vrijednost za  $x_1$  i  $x_2$ :

Prvo skraćujemo kongruencije:

$$(A) \rightarrow 170 > 9 \rightarrow \text{mod}(170, 9) = 8 \implies 8x_1 \equiv 8 \pmod{9}$$

$$(B) \rightarrow 153 > 10 \rightarrow \text{mod}(153, 10) = 3 \implies 3x_2 \equiv 2 \pmod{10}$$

Odgovarajuće diofantove jednačine:

$$(A) \rightarrow 8x_1 + 9y = 8 \rightarrow NZD(8, 9) = 1, 1 \mid 8$$

$$(B) \rightarrow 3x_2 + 10y = 2 \rightarrow NZD(3, 10) = 1, 1 \mid 2$$

Nalazimo  $x_1$  i  $x_2$  tako da  $y \in Z$ , pri čemu ne moramo rješavati diofantove jednačine, već pogađamo vrijednosti. Dobijamo:

$$x_1 = 1$$

$$x_2 = 4$$

$$\text{Također } x_3 = 0$$

Pa je opće rješenje:

$$x \equiv 170 \cdot 1 + 153 \cdot 4 + 90 \cdot 0 \pmod{1530}$$

$$x \equiv 782 \pmod{1530}$$

Možemo pisati:

$$x = 782 + 1530t, t \in Z$$

Nalazimo tipično rješenje za koje vrijedi  $0 \leq x < 1530$

$$0 \leq 782 + 1530t < 1530$$

$$t \geq -\frac{782}{1530} \quad \wedge \quad t < \frac{748}{1530}$$

$$t \geq -0.51 \quad \wedge \quad t < 0.488$$

$$t \in [-0.51, 0.488) \wedge t \in \mathbb{Z} \implies \underline{t = 0}$$

Uvrštavanjem u  $x = 782 + 1530t$ , se dobije:

$$\underline{x = 782}$$

Zaključujemo da ne samo da je 782 minimalan broj banana potreban da se jednako rasporede u odgovarajuće gomile, već je to i jedini broj za koji može to da se uradi. Provjeriti ćemo rezultat vraćajući  $x$  u početne jednačine sistema:

$$782 \equiv 8 \pmod{9} \implies 782 + 9y = 8 \implies y \in \mathbb{Z}$$

$$782 \equiv 2 \pmod{10} \implies 782 + 10y = 2 \implies y \in \mathbb{Z}$$

$$782 \equiv 0 \pmod{17} \implies 782 + 17y = 0 \implies y \in \mathbb{Z}$$

Minimalan(i jedini) broj banana potrebnih da bi se jednako raspodijelili je 782.



### Zadatak 3

a)

Slova Y i G se ponavljaju najviše puta. Slovo Y se ponavlja 8 puta, a slovo G se ponavlja 6 puta u sifriranoj poruci. Pošto se u bosanskom jeziku najčešće pojavljuje slovo A, a nakon njega po učestanosti slovo E, možemo pretpostaviti da je prilikom šifriranja došlo do zamjene slova A slovom Y i slova E slovom G. Slova A, Y, E i G imaju ASCII vrijednosti respektivno: 65, 89, 69 i 71. Iz uslova zadatka imamo algoritam:

$$y = (\text{mod } ax + b, 26) + 65$$

Gdje je x ASCII kod slova koje se zamijeni ASCII kodom slova y. Dakle, iz navedene pretpostavke mora vrijediti:

$$89 = (\text{mod } a \cdot 65 + b, 26) + 65$$

$$71 = (\text{mod } a \cdot 69 + b, 26) + 65$$

Odnosno:

$$(\text{mod } 65 \cdot a + b, 26) = 24$$

$$(\text{mod } 69 \cdot a + b, 26) = 6$$

Zapišimo ove jednačine u obliku kongruencija:

$$65 \cdot a + b \equiv 24 \pmod{26}$$

$$69 \cdot a + b \equiv 6 \pmod{26}$$

Oduzimanjem prve kongruencije od druge dobijemo kongruenciju:

$$4a \equiv -18 \pmod{26}$$

Odgovarajuća diofantova jednačina:

$$4a + 26k = -18, k \in \mathbb{Z}$$

$NZD(4, 26) = 2$ ,  $2 \mid 18$ , pa očekujemo 2 tipična rješenja. Dijelimo jednačinu sa 2:

$$2a + 13k = -9, k \in Z$$

$NZD(2, 13) = 1$ ,  $1 \mid 9$ , pa proširenim euklidovim algoritmom dobijamo  $1 = -6 \cdot 2 + 13$ . Pa je opće rješenje za  $a$ :

$$a = 54 + 13t, t \in Z$$

Za tipična rješenja mora vrijediti  $0 \leq a \leq 25$ . Pa se dobije da su tipična rješenja za  $t = -3$  i  $t = -4$ , i njihove vrijednosti:  $a = 15$  i  $a = 2$ . Dalje, da bi našli vrijednost za  $b$ , uzimamo kongruenciju  $65 \cdot a + b \equiv 24 \pmod{26}$

Za  $a = 15$  se dobije kongruencija  $b \equiv -951 \pmod{26}$  iz koje slijedi  $b = -951 + 26t, t \in Z$

Za  $a = 2$  se dobije kongruencija  $b \equiv -106 \pmod{26}$  iz koje slijedi  $b = -106 + 26t, t \in Z$

Za tipična rješenja mora vrijediti  $0 \leq b \leq 25$ . Pa su za  $b$  tipična rješenja data sa  $t = 37$  za  $a = 15$  i  $t = 5$  za  $a = 2$ . Tj. vrijednosti tipičnih rješenja su  $b = 11$  i  $b = 24$ . Dakle, kao što je očekivano dobili smo 2 tipična rješenja:

$$a = 15, b = 11$$

$$a = 2, b = 24$$

Zaključujemo da postoje dva moguća rješenja za  $a$  i  $b$  kojim se  $A$  preslikava u  $Y$  i  $E$  preslikava u  $G$ . Možemo odbaciti drugi slučaj kada je  $a = 2$  i  $b = 24$  jer kada uvrstimo u jednačinu dobije se  $y = (\text{mod } 2x + 24, 26) + 65$ . Dakle,  $2x + 24$  je uvijek paran broj pa je i  $(\text{mod } 2x + 24, 26)$  uvijek paran, a suma parnog i neparnog broja daju neparan broj, pa  $y$  bude na kraju neparan. To znači da bi poruka morala sadržavati znakove sa neparnim ASCII kodovima, a očigledno to nije slučaj (npr slovo  $G$  ima ASCII kod 68). Dakle, uzimamo  $a = 15$  i  $b = 11$ .

b)

Funkcija šifriranja glasi:

$$y = (\text{mod } 15x + 11, 26) + 65$$

Potrebno je riješiti ovaj izraz uz uvjet  $65 \leq x < 91$  jer je to raspon za koje ASCII kodovi daju velika slova. Da bi računanje bilo lakše uzimamo smjenu  $x = 65 + x'$ , pa uvjet postane  $0 \leq x' < 26$ . Tj. sveli smo na traženje tipičnih rješenja za  $x'$ . Prvo izrazimo funkciju šifriranja tako da figuriše  $x'$ :

$$y = (\text{mod } 15x + 11, 26) + 65$$

$$y = (\text{mod } 15(65 + x') + 11, 26) + 65$$

$$y = (\text{mod } 986 + 15x', 26) + 65 \rightarrow y = (\text{mod } 15x' + 24, 26) + 65$$

Jer  $(\text{mod } 986, 26) = 24$ . Sada je potrebno izraziti  $x'$ . Napišimo formulu kao kongruenciju:

$$y - 65 = (\text{mod } 15x' + 24, 26) \implies y - 65 \equiv 15x' + 24 \pmod{26}$$

Pa izrazimo  $x'$ :

$$15x' \equiv y - 89 \pmod{26}$$

Gdje je  $x'$  nepoznata, a  $y$  parametar. Odgovarajuća diofantova jednačina je  $15x' + 26k = y - 89$ ,  $k \in \mathbb{Z}$ .  $\text{NZD}(15, 26) = 1$ ,  $1 \mid (y - 89)$ , pa je jednačina rješiva za svako  $y \in \mathbb{Z}$ . Primjenom proširenog euklidovog algoritma dobijemo:  $1 = 7 \cdot 15 - 4 \cdot 26$ .

Pa je opće rješenje za  $x'$

$$x' = 7y - 623 + 26t, t \in \mathbb{Z}$$

Sada je potrebno birati  $t$  tako da vrijedi  $0 \leq x' < 26$ . Jednostavniji način je da se zapiše dobiveni izraz kao kongruencija:

$$x' \equiv -623 + 7y \pmod{26}$$

Redukcijom koeficijenata po modulu 26 dobijamo:

$$x' \equiv -25 + 7y \pmod{26}$$

Pa je  $x' \equiv (-25 + 7y, 26)$ . Pošto je  $x = x' + 65$ , funkcija za dešifrovanje glasi:

$$x = (-25 + 7y, 26) + 65$$

c)

I zaista, za  $y = 89$  (slovo Y), funkcija daje vrijednost  $x = 65$  (slovo A), i za  $y = 71$  (slovo G),  $x = 69$  (slovo E).

Listing funkcije u C++-u koja vraća dešifriranu poruku na osnovu one koja je vraćena kao parametar, pomoću dobivene funkcije dešifriranja je data ispod:

---

```

1 string Desifruj(string sif, string desif=""){
2     for(int i = 0; i < sif.size(); i++)
3         desif += ((-25+7*(int)(sif[i] - '\0'))%26+65) - '\0';
4     return desif;
5 }
```

---

Dešifrovana poruka glasi:

DISKRETNAMATEMATIKANIJETESKANIZAKOGAKOVJEZBAREDOVNO

Ako dodamo razmake:

DISKRETNAMATEMATIKA NIJE TESKA NI ZAKOGAKOVJEZBA  
REDOVNO

## Zadatak 4

a)

$$8x + 10y + 17z \equiv 64 \pmod{93} \quad (1)$$

$$12x + 9y + 19z \equiv 3 \pmod{93} \quad (2)$$

$$7x + 14y + 15z \equiv 68 \pmod{93} \quad (3)$$

Množimo kongruenciju 1 sa 12 i kongruenciju 2 sa -8, te ih sabiramo. To ima smisla uraditi jer je  $NZD(93, 12) = 1 \wedge NZD(93, 8) = 1$ . Dakle dobijamo:

$$48y + 52z \equiv 744 \pmod{93}$$

Pošto  $744 > 93 \implies \text{mod}(744, 93) = 0$ , kongruencija se svede na:

$$48y + 52z \equiv 0 \pmod{93}$$

Dalje, množimo kongruenciju 2 sa 7 i kongruenciju 3 sa -12, te ih sabiramo. NZD u oba slučaja je 1. Dobijamo:

$$105y + 47z \equiv 795 \pmod{93}$$

Daljim skraćivanjem se dobije:

$$12y + 47z \equiv 51 \pmod{93}$$

Sistem smo sveli na sljedeće tri kongruencije:

$$48y + 52z \equiv 0 \pmod{93}$$

$$12y + 47z \equiv 51 \pmod{93}$$

$$7x + 14y + 15z \equiv 68 \pmod{93}$$

Množimo prvu kongruenciju sa -47 i drugu kongruenciju sa 52, sabiramo ih, skratimo, te dobijemo kongruenciju sa jednom nepoznatom:

$$-51y \equiv 48 \pmod{93}$$

Odgovarajuća diofantova jednačina je  $-51y + 93k = 48$  gdje je  $k$  parametar,  $k \in \mathbb{Z}$ . Pošto je  $NZD(93, 51) = 3 \wedge 3 \mid 48$ , diofantova jednačina je rješiva, te očekujemo 3 tipična rješenja. Proširenim euklidovim algoritmom se dobije:

$$1 = 11 \cdot 17 - 6 \cdot 31$$

Interesuje nas rješenje po promjenljivoj  $y$ :

$$y = -176 + 31t$$

Za tipična rješenja mora vrijediti:  $0 \leq y \leq 92 \rightarrow t \in [6, 8]$ . Dakle dobili smo 3 tipična rješenja koja glase:

$$y = 10, y = 41, y = 72$$

Za  $y = 10$  kongruencija ima najmanje tipično rješenje, pa opće rješenje možemo pisati u obliku  $y \equiv 10 \pmod{31}$ . Da ne bi razmatrali svaki od tipičnih rješenja zasebno, možemo na sljedeći način napisati opće rješenje:

$$y = 10 + 31t, t \in \mathbb{Z}$$

Dobiveno opće rješenje vraćamo u prvu kongruenciju:

$$48(10 + 31t) + 52z = 0 \pmod{93}$$

Tj. skraćivanjem:

$$52z = -15 \pmod{93}$$

Pa je odgovarajuća diofantova jednačina  $52z + 93k = -15, k \in Z$ .  $NZD(93, 520) = 1 \wedge 1 \mid 15$ , dakle diofantova jednačina je rješiva te očekujemo jedinstveno tipično rješenje. Dobije se  $z = -510 + 93t, t \in Z$ . Pa je tipično rješenje:

$$z = 48 \rightarrow z \equiv 48 \pmod{93}$$

Uvrštavamo  $z = 48$  i  $y = 10 + 31t, t \in Z$  u kongruenciju 3. Dobije se:

$$7x = -48 - 62t \pmod{93}, t \in Z$$

Odgovarajuća diofantova jednačina:  $7x + 93k = -48 - 62t, t, k \in Z$ . Diofantova jednačina je rješiva, te očekujemo jedno tipično rješenje za svaki cijeli broj  $t$ ,  $NZD(93, 7) = 1 \wedge 1 \mid -48 - 62t$ . Dobije se  $x = -672 - 868t + 93s, t, s \in Z$ . Pa je  $s = 8 + \frac{868}{93} \cdot t, t \in Z$ . Tipično rješenje je jedinstveno i ono glasi:

$$x = 72 - 868t, t \in Z \rightarrow x \equiv 72 - 31t \pmod{93}$$

Dakle, rješenja sistema su:

$$x \equiv 72 - 31t \pmod{93}, t \in Z$$

$$y \equiv 10 \pmod{31}$$

$$z \equiv 48 \pmod{93}$$

Pri čemu svako tipično rješenje koje smo dobili za  $y$  odgovara da bude rješenje sistema. Dakle, ovaj sistem ima 3 tipična rješenja:

$$x = 310, y = 10, z = 48$$

$$x = 1271, y = 41, z = 48$$

$$x = 2232, y = 72, z = 48$$

b)

$$24x + 27y \equiv 9 \pmod{78} \quad (1)$$

$$10x + 12y \equiv 16 \pmod{78} \quad (2)$$

Ne možemo množiti kongruencije odgovarajućim brojevima jer njihovi odgovarajući  $NZD \neq 1$ . Dakle, moramo postepeno smanjivati koeficijent uz neku nepoznatu u nekoj kongruenciji, dok ne nestane potpuno. Uradit ćemo sljedeće korake, kako bi nepoznatu  $x$  izbacili iz druge kongruencije:

- 1.) Množimo kongruenciju 2 sa -1 i dodajemo kongruenciji 1. Ovaj korak uradimo 2 puta uzastopno.
- 2.) Množimo kongruenciju 1 sa -1 i dodajemo kongruenciji 2. Ovaj korak uradimo 2 puta uzastopno također.
- 3.) Uradimo 1. ponovno, ali ovaj put samo jednom.
- 4.) Uradimo 2. ponovno, ali ovaj put samo jednom.

Dobili smo sistem:

$$2x - 3y \equiv -85 \pmod{78}$$

$$9y \equiv 147 \pmod{78}$$

Sistem sa jednom nepoznatom svodimo na diofantovu jednačinu  $9y + 78k = 147$ , gdje je  $k$  parametar.  $NZD(78, 9) = 3 \wedge 3 \mid 69$ . Zaključujemo da je diofantova jednačina rješiva, i očekujemo 3 tipična rješenja. Podijelimo diofantovu jednačinu sa 3, dobijamo  $3y + 26k = 23$ . Proširenim euklidovim algoritmom dobijemo  $1 = 9 \cdot 3 - 1 \cdot 26$ . Pa je  $y = 207 + 26t, t \in \mathbb{Z}$ . Za  $t = -7, t = -6, t = -5$  dobijamo tipična rješenja ove kongruencije:

$$y = 25, y = 51, y = 77$$

Najmanje tipično rješenje je  $y = 25$ , pa možemo također pisati:

$$y \equiv 25 \pmod{26}$$



Da ne bi morali za svako tipično rješenje računati sistem, pišemo općenito  $y = 25 + 26t, t \in \mathbb{Z}$ . Isti izraz vraćamo u prvu kongruenciju tj.

$$\begin{aligned} 2x - 3y &\equiv -85 \pmod{78} \rightarrow 2x \equiv -10 + 78t \pmod{78} \\ 2x &\equiv -10 \pmod{78} \end{aligned}$$

Odgovarajuća diofantova jednačina je  $2x + 78k = -10$ , gdje je  $k$  parametar.  $NZD(78, 2) = 2 \wedge 2 \mid 10$ , dakle diofantova jednačina je rješiva i očekujemo 2 tipična rješenja. Rješenje diofantove jednačine je  $x = -5 + 39t, t \in \mathbb{Z}$ . Iz rješenja slijedi da za  $t = 1 \wedge t = 2$  imamo tipična rješenja:

$$x = 34, x = 73$$

Najmanje tipično rješenje je  $x = 34$ , pa možemo također pisati:

$$x \equiv 34 \pmod{39}$$

Zaključujemo da je rješenje sistema:

$$\begin{aligned} x &\equiv 34 \pmod{39} \\ y &\equiv 25 \pmod{26} \end{aligned}$$

Ili zapisano u vidu tipičnih rješenja; ovaj sistem ima 6 tipičnih rješenja:

$$\begin{aligned} x = 34, y = 25; x = 34, y = 51; x = 34, y = 77 \\ x = 73, y = 25; x = 73, y = 51; x = 73, y = 77 \end{aligned}$$

## Zadatak 5

a)

$$x^2 \equiv 212 \pmod{2093}$$

$m = 2093$  nije prost broj, ali je neparan, tako da svakako vrijede pravila računa sa Legendreovim simbolom (tkz. Legendre-Jacobijev simbol). Pošto vrijedi:

$$NZD(212, 2093) = 1 \wedge 2093 = 2^0 \cdot 7 \cdot 13 \cdot 23$$

uvjeti rješivosti zadane kvadratne kongruencije su:

$$(212 \mid 7) = 1$$

$$(212 \mid 13) = 1$$

$$(212 \mid 23) = 1$$

Pošto je  $e = 0$ , nema dopunskih uvjeta. Provjerimo uvjete rješivosti:

$$(212 \mid 7) = (\text{mod}(212, 7) \mid 7) = (2 \mid 7) = (-1)^{\frac{49-1}{8}} = (-1)^6 = 1$$

$$(212 \mid 13) = (\text{mod}(212, 13) \mid 13) = (4 \mid 13) = (2^2 \mid 13) = 1$$

$$\begin{aligned} (212 \mid 23) &= (\text{mod}(212, 23) \mid 23) = (5 \mid 23) = (23 \mid 5) \cdot (-1)^{\frac{4 \cdot 22}{4}} = \\ &= (23 \mid 5) = (\text{mod}(23, 5) \mid 5) = (3 \mid 5) = (5 \mid 3) \cdot (-1)^{\frac{2 \cdot 4}{4}} = (5 \mid 3) = \\ &= (\text{mod}(5, 3) \mid 3) = (2 \mid 3) = (-1)^{\frac{9-1}{8}} = -1 \end{aligned}$$

Primjetimo da uvjet  $(212 \mid 23) \neq 1$  pa zadana kvadratna kongruencija nije rješiva.

b)

$$x^2 \equiv 1033 \pmod{1368}$$

U ovom slučaju vrijedi:

$$NZD(1033, 1368) = 1 \wedge 1368 = 2^3 \cdot 3^2 \cdot 19$$

Uvjeti rješivosti ove kvadratne kongruencije su:

$$(1033 \mid 3) = 1$$

$$(1033 \mid 19) = 1$$

Dalje, pošto je  $e = 3 (\geq 3)$  imamo dopunski uvjet  $a \equiv 1 \pmod{8}$ . Dopunski uvjet je ispunjen jer  $\text{mod}(1033, 8) = 1$ . Ispitajmo ostale uvjete:

$$(1033 \mid 3) = (\text{mod}(1033, 3) \mid 3) = (1 \mid 3) = 1$$

$$\begin{aligned} (1033 \mid 19) &= (\text{mod}(1033, 19) \mid 19) = (7 \mid 19) = (19 \mid 7) \cdot (-1)^{\frac{18 \cdot 6}{4}} = \\ &= -(5 \mid 7) = -(7 \mid 5) \cdot (-1)^{\frac{6 \cdot 4}{4}} = -(2 \mid 5) = -(-1)^{\frac{24}{8}} = 1 \end{aligned}$$

Zaključujemo da je kvadratna kongruencija rješiva, te je njen broj rješenja:

$$2^{k+2} = 2^{2+2} = 2^4 = 16$$

c)

$$x^2 \equiv 919 \pmod{120}$$

Skraćivanjem koeficijenta dobijemo:

$$x^2 \equiv 79 \pmod{120}$$

Za ovaj slučaj vrijedi:

$$NZD(79, 120) = 1 \wedge 120 = 2^3 \cdot 3 \cdot 5$$

Očigledno je  $e = 3$ , pa su uvjeti rješivosti:

$$(79 \mid 3) = 1$$

$$(79 \mid 5) = 1$$

$$\text{dopunski uvjet: } a \equiv 1 \pmod{8} \implies 79 \equiv 1 \pmod{8}$$

Prva dva uvjeta su zadovoljena:

$$(79 \mid 3) = (\text{mod}(79, 3) \mid 3) = (1 \mid 3) = 1$$

$$(79 \mid 5) = (\text{mod}(79, 5) \mid 5) = (4 \mid 5) = (2^2 \mid 5) = 1$$

Međutim, dopunski uvjet nije zadovoljen jer  $\text{mod}(79, 8) = 7 \neq 1$ . Dakle, ova kvadratna kongruencija nije rješiva.

d)

$$x^2 \equiv 375 \pmod{40425}$$

U ovom slučaju  $NZD(375, 40425) = 75 \neq 1$ , dakle kvadratna kongruencija je rješiva akko vrijedi  $NZD(\frac{a}{q^2}, \frac{m}{d}) = 1$  i ako je rješiva kvadratna kongruencija  $y^2 \equiv \frac{a}{q^2} \pmod{\frac{m}{d}}$ . Gdje vrijedi  $d = p \cdot q^2$ . Konkretno, u ovom slučaju je:

$$75 = 3 \cdot 5^2 \rightarrow p = 3 \wedge q = 5$$

Pa imamo da je  $NZD(15, 539) = 1$ , pa je prvi uslov zadovoljen. Provjeravamo da li je kvadratna kongruencija po  $y$  rješiva. Imamo da je:

$$y^2 \equiv 15 \pmod{539}$$

Rastavljanjem na proste faktore dobijemo  $539 = 2^0 \cdot 7^2 \cdot 11$ . Dakle, kvadratna kongruencija je rješiva ako su ispunjeni uslovi:

$$(15|7) = 1$$

$$(15|11) = 1$$

Ispitajmo:

$$(15|7) = (\text{mod}(15, 7)|7) = (1|7) = 1$$

$$(15|11) = (\text{mod}(15, 11)|11) = (4|11) = (2^2|11) = 1$$

Pa je kvadratna kongruencija rješiva, te je potrebno odrediti broj rješenja kvadratne kongruencije po  $y$ , a pošto je  $e = 0$ , broj rješenja je:

$$n = 2^k = 2^2 = 4$$

Konačno, broj rješenja početne kvadratne kongruencije je:

$$n \cdot q = 4 \cdot 5 = 20$$

## Zadatak 6

Pretpostavimo da su sve kvadratne kongruencije rješive.

a)

$$[64]_{89} \rightarrow x^2 \equiv 64 \pmod{89}$$

$p = 89$  je prost broj različit od 2. Pošto je  $\text{mod}(89, 4) = \text{mod}(89, 8) = 1$ , koristimo Tonelli algoritam. Potrebno je naći broj  $g$  takav da  $(g \mid 89) = -1$ .

Probajmo za  $g = 2$

$$(2 \mid 89) = (-1)^{990} = 1$$

Uvjet nije zadovoljen, probajmo sa  $g = 3$

$$(3 \mid 89) = (89 \mid 3)(-1)^{\frac{88 \cdot 2}{4}} = (89 \mid 3)(-1)^{44} = (\text{mod}(89, 3) \mid 3) = (2 \mid 3) = -1$$

Uslov je zadovoljen,  $g = 3$ . Potrebno je još izračunati broj  $h = \text{inv}(g, p) = \text{inv}(3, 89) = ([3]_{89})^{-1}$

$$([3]_{89})^{-1} \rightarrow 3x \equiv 1 \pmod{89} \rightarrow 3x + 89y = 1$$

Gdje je  $y$  parametar. Prošireni euklidov algoritam daje rastavu  $1 = 3 \cdot 30 - 1 \cdot 89$  od čega slijedi  $x = 30 + 89t, t \in \mathbb{Z}$

$t = 0 \rightarrow x = 30$  tj.  $h = 30$ . Na kraju, potrebne varijable za Tonelli algoritam su:

$$t = \frac{89 - 1}{2} = 44, v = 1, w = 64, h = 30, g = 3, p = 89$$

Nakon prvog prolaska kroz petlju:

$$t = 22, h = 10, g = 9$$

Nakon drugog tj. posljednjeg prolaska kroz petlju:

$$t = 11, h = 11, g = 81$$

Pa su konačna rješenja:

$$x = \text{mod}(64^6, 89) = 8$$

$$x = 89 - 8 = 81$$

b)

$$[85]_{1369} \rightarrow x^2 \equiv 85 \pmod{1369}$$

$m = 1369$  nije prost broj, napišimo ga u obliku  $m = p^k$  tj.  $1369 = 37^2$ .

Dakle, rješavamo kongruenciju  $x^2 \equiv 85 \pmod{37}$ .  $p = 37$  je prost broj za koji vrijedi:

$$\text{mod}(37, 4) \neq 3$$

$$\text{mod}(37, 8) = 5$$

Pa je jedno tipično rješenje:

$$x = \text{mod}(a^{\frac{p+3}{8}} \cdot 2^{\frac{p-1}{4}}, p)$$

$$x = \text{mod}(11^5 \cdot 2^9, 37)$$

$$x = 23 (= x_1)$$

Da bi dobili rješenje početne kvadratne kongruencije, potrebno je izračunati:

$$[h]_p = ([2 \cdot x_1]_p)^{-1} = ([46]_{37})^{-1}$$

Odgovarajuća diofantova jednačina je  $46h + 37y = 1$ . Prošireni euklidov algoritam daje rastavu  $1 = 5 \cdot 37 - 4 \cdot 46$ .

Iz čega slijedi  $h = -4 + 37t, t \in \mathbb{Z} \rightarrow t = 1 \rightarrow \underline{h = 33}$ . Koristimo rekursivnu formulu da izračunamo jedno tipično rješenje:

$$\begin{aligned}x_2 &= \text{mod}(x_1 - h((x_1)^2 - a), p^2) \\x_2 &= \text{mod}(23 - 33(23^2 - 85), 37^2) \\x_2 &= 939\end{aligned}$$

Zaključujemo da su rješenja:

$$\begin{aligned}x &= 939 \\x &= 1369 - 939 = 430\end{aligned}$$

c)

$$[9]_{133} \rightarrow x^2 \equiv 9 \pmod{133}$$

$m = 133$  je složen broj. Rastavimo na proste faktore  $133 = 7 \cdot 19$ , pa je zadana kongruencija ekvivalentna sljedećem sistemu kongruencija:

$$\begin{aligned}x^2 &\equiv 9 \pmod{7} \\x^2 &\equiv 9 \pmod{19}\end{aligned}$$

Rješavamo zasebno obje kvadratne kongruencije. Za prvu kvadratnu kongruenciju vrijedi  $\text{mod}(7, 4) = 3$ , pa su njena tipična rješenja:

$$\begin{aligned}x &= \text{mod}(a^{\frac{p+1}{4}}, p) = \text{mod}(9^2, 7) = 4 \\x &= p - 4 = 7 - 4 = 3\end{aligned}$$

Za drugu kvadratnu kongruenciju vrijedi također  $\text{mod}(19, 4) = 3$ , pa su njena tipična rješenja:



$$x = 16$$

$$x = 3$$

Možemo formirati četiri sistema od dvije linearne kongruencije koje figurisu dobivena tipična rješenja:

$$x \equiv 4 \pmod{7}, x \equiv 16 \pmod{19} \quad (1)$$

$$x \equiv 3 \pmod{7}, x \equiv 16 \pmod{19} \quad (2)$$

$$x \equiv 4 \pmod{7}, x \equiv 3 \pmod{19} \quad (3)$$

$$x \equiv 3 \pmod{7}, x \equiv 3 \pmod{19} \quad (4)$$

Koristit ćemo kinesku teoremu o ostacima za rješavanje svih sistema. To smijemo uraditi jer  $NZD(7, 19) = 1$ . Također, za sva 4 sistema vrijedi sljedeće:

$$n_1 \cdot n_2 = 133$$

$$\lambda_1 = \frac{133}{7} = 19$$

$$\lambda_2 = \frac{133}{19} = 7$$

$$x = 19x_1 + 7x_2 \pmod{133}$$

Rješavamo prvi sistem:

$$19x_1 \equiv 4 \pmod{7}$$

$$7x_2 \equiv 16 \pmod{19}$$

Rješavamo obje kongruencije uporedo. Odgovarajuće diofantove jednačine:

$$19x_1 + 7y = 4$$

$$7x_2 + 19y = 16$$

Gdje je  $y$  parametar. Prošireni euklidov algoritam daje rastavu:

$$1 = 3 \cdot 19 - 8 \cdot 7$$

Dobivena jednakost vrijedi za obje jednačine, pa je:

$$\begin{aligned}x_1 &= 12 + 7t, t \in Z \rightarrow t = -1 \rightarrow \underline{x_1 = 5} \\x_2 &= -128 + 19t, t \in Z \rightarrow t = 7 \rightarrow \underline{x_2 = 5}\end{aligned}$$

Na kraju, rješenje prvog sistema je:

$$\begin{aligned}x &\equiv 19 \cdot 5 + 7 \cdot 5 \pmod{133} \\x &\equiv 130 \pmod{133} \\x &= \underline{130}\end{aligned}$$

Rješavamo drugi sistem:

$$\begin{aligned}19x_1 &\equiv 3 \pmod{7} \\7x_2 &\equiv 16 \pmod{19}\end{aligned}$$

Druga kongruencija je riješena u prethodnom slučaju,  $\underline{x_2 = 5}$ . Odgovarajuća diofantova jednačina je ista kao i u prethodnom slučaju. Lahko zaključujemo da vrijedi:

$$x_1 = 9 + 7t, t \in Z \rightarrow t = -1 \rightarrow \underline{x_1 = 2}$$

Rješenje drugog sistema je:

$$\begin{aligned}x &\equiv 19 \cdot 2 + 7 \cdot 5 \pmod{133} \\x &\equiv 73 \pmod{133} \\x &= \underline{73}\end{aligned}$$

Rješavamo treći sistem:

$$19x_1 \equiv 4 \pmod{7}$$

$$7x_2 \equiv 3 \pmod{19}$$

Prva kongruencija je riješena ranije  $x_1 = 5$ , diofantova jednačina je ista kao i tokom rješavanja prvog sistema. Dakle:

$$x_2 = -24 + 19t, t \in \mathbb{Z} \rightarrow t = 2 \rightarrow \underline{x_2 = 14}$$

Rješenje trećeg sistema:

$$x \equiv 19 \cdot 5 + 7 \cdot 14 \pmod{133}$$

$$x \equiv 196 \pmod{133}$$

$$x \equiv 60 \pmod{133}$$

$$\underline{x = 60}$$

Rješavamo četvrti sistem:

$$19x_1 \equiv 3 \pmod{7}$$

$$7x_2 \equiv 3 \pmod{19}$$

Obje kongruencije su riješene u prethodnim sistemima, dakle slijedi:

$$\underline{x_1 = 2} \wedge \underline{x_2 = 14}$$

Rješenje četvrtog sistema je:

$$x \equiv 19 \cdot 2 + 7 \cdot 14 \pmod{133}$$

$$x \equiv 136 \pmod{133}$$

$$x \equiv 3 \pmod{133}$$

$$\underline{x = 3}$$

Rješenja polazne kvadratne kongruencije su:

$$x = 3$$

$$x = 60$$

$$x = 73$$

$$x = 130$$

d)

$$[1431]_{5643} \rightarrow x^2 \equiv 1431 \pmod{5643}$$

Pošto je  $NZD(1431, 5643) = 27 = 3^3$ , transformišemo kvadratnu kongruenciju. Napišimo  $d = 27$  u obliku  $d = d \cdot q^2 \rightarrow 27 = 3 \cdot 3^2$ . Dakle, uvrstimo smjenu  $x = 9y$ . Polazna kongruencija postaje:

$$81y^2 \equiv 1431 \pmod{5643}$$

Dijelimo sa 27:

$$3y^2 \equiv 53 \pmod{209}$$

Smjena  $y^2 = z$ :

$$3z \equiv 53 \pmod{209}$$

Dobivena linearna kongruencija je rješiva jer  $NZD(3, 209) = 1 \wedge 1 \mid 53$ . Odgovarajuća diofantova jednačina je  $3z + 209u = 53$ . Prošireni euklidov algoritam daje rastavu  $1 = -209 + 3 \cdot 70$  tj.  $z = 3710 + 209t, t \in \mathbb{Z}$ . Iz čega slijedi  $t = -17 \rightarrow \underline{z = 157}$ . Dakle:

$$z \equiv 157 \pmod{209}$$

Vratimo smjenu:

$$y^2 \equiv 157 \pmod{209}$$

$NZD(157, 209) = 1$  što smo i htjeli postići. Broj  $m = 209$  je složen, rastavimo na proste faktore  $209 = 11 \cdot 19$ . Dakle, dobivena kvadratna kongruencija je ekvivalentna sljedećem sistemu:

$$y^2 \equiv 157 \pmod{11} \rightarrow y^2 \equiv 3 \pmod{11}$$

$$y^2 \equiv 157 \pmod{19} \rightarrow y^2 \equiv 5 \pmod{19}$$

Kongruencije su proste, njihova rješenja su, respektivno:

$$y = 5, y = 6$$

$$y = 9, y = 10$$

Kao i u prethodnom zadatku, dobili smo četiri sistema od po dvije linearne kongruencije:

$$y \equiv 5 \pmod{11}, y \equiv 9 \pmod{19} \tag{1}$$

$$y \equiv 6 \pmod{11}, y \equiv 9 \pmod{19} \tag{2}$$

$$y \equiv 5 \pmod{11}, y \equiv 10 \pmod{19} \tag{3}$$

$$y \equiv 6 \pmod{11}, y \equiv 10 \pmod{19} \tag{4}$$

Možemo sve sisteme riješiti kineskom teoremom o ostacima, to smijemo uraditi jer  $NZD(11, 19) = 1$ . Za sve sisteme vrijedi sljedeće:

$$n_1 \cdot n_2 = 209$$

$$\lambda_1 = \frac{209}{11} = 19$$

$$\lambda_2 = \frac{209}{19} = 11$$

$$y = 19y_1 + 11y_2 \pmod{209}$$

Rješavamo prvi sistem:

$$19y_1 \equiv 5 \pmod{11}$$

$$11y_2 \equiv 9 \pmod{19}$$

Rješavamo obje kongruencije uporedo. Odgovarajuće diofantove jednačine:

$$19y_1 + 11u = 5$$

$$11y_2 + 19u = 9$$

Gdje je  $u$  parametar. Prošireni euklidov algoritam daje rastavu:

$$1 = 7 \cdot 11 - 4 \cdot 19$$

Dobivena jednakost vrijedi za obje jednačine, pa je:

$$y_1 = -20 + 11t, t \in Z \rightarrow t = 2 \rightarrow \underline{y_1 = 2}$$

$$y_2 = 63 + 19t, t \in Z \rightarrow t = -3 \rightarrow \underline{y_2 = 6}$$

Na kraju, rješenje prvog sistema je:

$$x \equiv 19 \cdot 2 + 11 \cdot 6 \pmod{209}$$

$$x \equiv 104 \pmod{209}$$

$$\underline{y = 104}$$

Rješavamo drugi sistem:

$$19y_1 \equiv 6 \pmod{11}$$

$$11y_2 \equiv 9 \pmod{19}$$

Druga kongruencija je riješena u prethodnom slučaju,  $y_2 = 6$ . Odgovarajuća diofantova jednačina je ista kao i u prethodnom slučaju. Lahko zaključujemo da vrijedi:

$$y_1 = -24 + 11t, t \in \mathbb{Z} \rightarrow t = 3 \rightarrow \underline{y_1 = 9}$$

Rješenje drugog sistema je:

$$y \equiv 19 \cdot 9 + 11 \cdot 6 \pmod{209}$$

$$y \equiv 237 \pmod{209}$$

$$y \equiv 28 \pmod{209}$$

$$\underline{y = 28}$$

Rješavamo treći sistem:

$$19y_1 \equiv 5 \pmod{11}$$

$$11y_2 \equiv 10 \pmod{19}$$

Prva kongruencija je riješena ranije  $y_1 = 2$ , diofantova jednačina je ista kao i tokom rješavanja prvog sistema. Dakle:

$$y_2 = 70 + 19t, t \in \mathbb{Z} \rightarrow t = -3 \rightarrow \underline{y_2 = 13}$$

Rješenje trećeg sistema:

$$y \equiv 19 \cdot 2 + 11 \cdot 13 \pmod{209}$$

$$y \equiv 181 \pmod{209}$$

$$\underline{y = 181}$$

Rješavamo četvrti sistem:

$$19y_1 \equiv 6 \pmod{11}$$

$$11y_2 \equiv 10 \pmod{19}$$

Obje kongruencije su riješene u prethodnim sistemima, dakle slijedi:

$$\underline{y_1 = 9} \wedge \underline{y_2 = 13}$$

Rješenje četvrtog sistema je:

$$y \equiv 19 \cdot 9 + 13 \cdot 11 \pmod{209}$$

$$y \equiv 314 \pmod{209}$$

$$y \equiv 105 \pmod{209}$$

$$\underline{y = 105}$$

Rješenja svih sistema su, respektivno:

$$\underline{y = 104}, \underline{y = 28}, \underline{y = 181}, \underline{y = 105}$$

Tj.:

$$y \equiv 104 \pmod{209}$$

$$y \equiv 28 \pmod{209}$$

$$y \equiv 181 \pmod{209}$$

$$y \equiv 105 \pmod{209}$$

Pošto je  $x = 9y$ , ova rješenja postaju:



$$x \equiv 936 \pmod{1881}$$

$$x \equiv 252 \pmod{1881}$$

$$x \equiv 1629 \pmod{1881}$$

$$x \equiv 945 \pmod{1881}$$

U zadatku su traženi diskretni kvadratni korijeni koji su zapravo tipična rješenja tj. rješenja u opsegu  $0 \leq x < 5643 \rightarrow 0 \leq x \leq 5642$ . Dakle, za svaku dobivenu kongruenciju računamo diskretne kvadratne korijene tj. računamo njihova rješenja u spomenutom opsegu. To ćemo uraditi uzastopno.

Odgovarajuće diofantove jednačine:

$$x + 1881u = 936$$

$$x + 1881u = 252$$

$$x + 1881u = 1629$$

$$x + 1881u = 945$$

Odgovarajuća rješenja:

$$x = 936 + 1881t, t \in \mathbb{Z}$$

$$x = 252 + 1881t, t \in \mathbb{Z}$$

$$x = 1629 + 1881t, t \in \mathbb{Z}$$

$$x = 945 + 1881t, t \in \mathbb{Z}$$

Kada sva rješenja stavimo u opseg  $0 \leq x \leq 5642$  dobijemo:

$$x = 936, x = 2817, x = 4698$$

$$x = 252, x = 2133, x = 4014$$

$$x = 1629, x = 3510, x = 5391$$

$$x = 945, x = 2826, x = 4707$$

Ovo su rješenja početne kvadratne kongruencije, ima ih 12. Konačno, sortirajmo ih u rastući poredak:

$$x = 252$$

$$x = 936$$

$$x = 945$$

$$x = 1629$$

$$x = 2133$$

$$x = 2817$$

$$x = 2826$$

$$x = 3510$$

$$x = 4014$$

$$x = 4698$$

$$x = 4707$$

$$x = 5391$$

## Zadatak 7

### Postavka:

Ana i Bakir žele da razmjenjuju poruke šifrirane nekim algoritmom koji zahtijeva tajni ključ, ali nemaju sigurnog kurira preko kojeg bi mogli preneti 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  $p = 881$  i generator  $g = 13$ . Nakon toga, Ana je u tajnosti slučajno izabrala broj  $a = 271$ , dok se Bakir u tajnosti odlučio za broj  $b = 172$ . Odredite koje još informacije Ana i Bakir moraju razmijeniti preko ETF Haber kutije da bi se dogovorili o vrijednosti ključa, te kako glasi ključ koji su oni dogovorili.

### Rješenje:

Pošto imamo sve potrebne informacije za računanje ključa po Diffie-Hellmanovom protokolu, možemo odmah preći na računanje istog.

Ana računa vrijednost:

$$\alpha = \text{mod}(g^a, p) = \text{mod}(13^{271}, 881) = ([13]_{881})^{271}$$

Napišimo broj 271 preko sume stepena dvojke.  $271 = 256 + 8 + 4 + 2 + 1$ . Tako da je:

$$([13]_{881})^{271} = ([13]_{881})^{256} \otimes ([13]_{881})^8 \otimes ([13]_{881})^4 \otimes ([13]_{881})^2 \otimes ([13]_{881})^1$$

Sada stepene računamo rekurzivno:

$$([13]_{881})^2 = [13^2]_{881} = [169]_{881}$$

$$([13]_{881})^4 = [169^2]_{881} = [28561]_{881} = [\text{mod}(28561, 881)]_{881} = [369]_{881}$$

$$([13]_{881})^8 = [369^2]_{881} = [487]_{881}$$

$$([13]_{881})^{256} = (([13]_{881})^8)^{32} = ([487]_{881})^{32} = ([487^4]_{881})^8 = ([684]_{881})^8 = [451]_{881}$$

Na kraju imamo:

$$([13]_{881})^{271} = [451]_{881} \otimes [487]_{881} \otimes [369]_{881} \otimes [169]_{881} \otimes [13]_{881} = [552]_{881}$$

Ana je izračunala vrijednost  $\underline{\alpha = 552}$  i šalje Bakiru (može i javno). Sada Bakir računa vrijednost:

$$\beta = \text{mod}(g^b, p) = \text{mod}(13^{172}, 881) = ([13]_{881})^{172}$$

Napišimo broj 172 preko sume stepena dvojke.  $172 = 128 + 32 + 8 + 4$ . Tako da je:

$$([13]_{881})^{172} = ([13]_{881})^{128} \otimes ([13]_{881})^{32} \otimes ([13]_{881})^8 \otimes ([13]_{881})^4$$

Stepene računamo rekurzivno, pri čemu ćemo samo napisati rezultate jer smo prethodno detaljnije:

$$\begin{aligned} ([13]_{881})^4 &= [369]_{881} \\ ([13]_{881})^8 &= [487]_{881} \\ ([13]_{881})^{32} &= [684]_{881} \\ ([13]_{881})^{128} &= [263]_{881} \end{aligned}$$

Na kraju imamo:

$$([13]_{881})^{172} = [877]_{881}$$

Bakir je izračunao vrijednost  $\underline{\beta = 877}$  i šalje je Ani (može javno također). Sada Ana u privatnosti računa ključ:

$$k = \text{mod}(\beta^a, p) = \text{mod}(877^{271}, 881) = ([877]_{881})^{271}$$

Prethodno smo opisali postupak računanja, sada napišimo  $271 = 256 + 8 + 4 + 2 + 1$ . I analogno kao u prethodnim slučajevima računamo stepene rekursivno i dobijemo:

$$([877]_{881})^{271} = [499]_{881}$$

Dakle, Ana je dobila ključ  $k = 499$ . Sada Bakir privatno računa ključ, mora dobiti istu vrijednost kao Ana. Bakir računa ključ po formuli:

$$k = \text{mod}(\alpha^b, p) = \text{mod}(552^{172}, 881) = ([552]_{881})^{172}$$

Dobijemo da je:

$$([552]_{881})^{172} = [499]_{881}$$

Tako da je i Bakir dobio ključ  $k = 499$ .

Zaključujemo da su Ana i Bakir morali razmijeniti informacije of brojevima  $\alpha = 552$  i  $\beta = 877$ . Također, ključ koji su dogovorili glasi  $k = 499$ .

## Zadatak 8

### Postavka:

Aida i Bogdan međusobno razmjenjuju poruke preko Facebook-a. Kako je poznato da takva komunikacija nije pouzdana, oni su odlučili da će primati samo šifrirane poruke. Aida je na svoj profil postavila informaciju da prima samo poruke šifrirane pomoću RSA kriptosistema s javnim ključem (535, 1363), dok je Bogdan postavio informaciju da prima samo poruke šifrirane RSA kriptosistemom s javnim ključem (73, 1271).

1. Odredite kako glase tajni ključevi koje koriste Aida i Bogdan za dešifriranje šifriranih poruka koje im pristižu.
2. Odredite kako glase funkcije šifriranja i dešifriranja koje koriste Aida i Bogdan za šifriranje poruka koje šalju jedno drugom, odnosno za dešifriranje šifriranih poruka koje im pristižu.
3. Odredite kako glasi šifrirana poruka  $y$  koju Aida šalje Bogdanu ako izvorna poruka glasi  $x = 6747$ . Kako glasi digitalni potpis  $z$  u slučaju da Aida želi Bogdanu dokazati da poruka potiče baš od nje?
4. Pokažite kako će Bogdan dešifrirati šifriranu poruku  $y$  koju mu je Aida poslala (tj. primijenite odgovarajuću funkciju za dešifriranje na šifriranu poruku) i na osnovu primljenog digitalnog potpisa  $z$  utvrditi da je poruka zaista stigla od Aide.

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

### Rješenje:

Javni ključevi dati u zadatku su oblika  $(a, m)$  tj. za Aidu:

$$a = 535, m = 1363$$

I za Bogdana:

$$a = 73, m = 1271$$

a)

Tajni ključ je par  $(b, m)$  gdje se  $b$  računa iz kongruencije:

$$ab \equiv 1 \pmod{\varphi(m)}$$

Za Aidu i Bogdana respektivno vrijedi:

$$\varphi(m) = \varphi(1363) = \varphi(29) \cdot \varphi(47) = 28 \cdot 46 = 1288$$

$$\varphi(m) = \varphi(1271) = \varphi(31) \cdot \varphi(41) = 30 \cdot 40 = 1200$$

Pa računamo sljedeće kongruencije:

$$535b \equiv 1 \pmod{1288}$$

$$73b \equiv 1 \pmod{1200}$$

Odgovarajuće diofantove jednačine:

$$535b + 1288u = 1$$

$$73b + 1200u = 1$$

Gdje je  $u$  parametar. Prošireni euklidov algoritam daje rastavu:

$$1 = -65 \cdot 535 + 27 \cdot 1288$$

$$1 = -263 \cdot 73 + 16 \cdot 1200$$

Opća rješenja za  $b$  su:

$$b = -65 + 1288t, t \in \mathbb{Z}$$

$$b = -263 + 1200t, t \in \mathbb{Z}$$

Pa su tipična rješenja:

$$t = 1 \rightarrow b = 1223$$

$$t = 1 \rightarrow b = 937$$

Tajni ključ za Aidu je (1223, 1363).

Tajni ključ za Bogdana je (937, 1271).

b)

Kada se poruke šalju Aidi, funkcija za šifriranje glasi:

$$E_A(x) = \text{mod}(x^{535}, 1363)$$

A kada se šalje Bogdanu, funkcija za šifriranje glasi:

$$E_B(x) = \text{mod}(x^{73}, 1271)$$

Za nalaženje funkcija dešifriranja  $D_A(y)$  i  $D_B(y)$  izračunali smo već tajne eksponente  $b_a = 1223$  i  $b_b = 937$ . Pa su odgovarajuće funkcije dešifriranja za Aidu i Bogdana respektivno:

$$D_A(y) = \text{mod}(y^{1223}, 1363)$$

$$D_B(y) = \text{mod}(y^{937}, 1271)$$

c)

Pošto Aida šalje Bogdanu, Aida će da koristi Bogdanovu funkciju za šifriranje  $E_B(x) = \text{mod}(x^{73}, 1271)$ . Međutim, pošto je  $x = 6747 > 1271$ , izrazit ćemo  $x$  u bazi 1271, te svaku 'cifru' posebno šifrirati. Broj 6747 napisan u bazi 1271 je  $6747 = 5 \cdot 1271 + 392$ . Dakle šifriramo 5 i 392.

$$E_B(5) = \text{mod}(5^{73}, 1271) = ([5]_{1271})^{73} = 408$$

$$E_B(392) = \text{mod}(392^{73}, 1271) = ([392]_{1271})^{73} = 72$$

Na kraju, šifrirana poruka glasi:  $y = 408 \cdot 1271 + 72 \implies \underline{y = 518640}$ . Digitalni potpis  $z$  računamo kao:

$$z = E_B(D_A(6747))$$



Prvo izračunajmo  $D_A(6747) = \text{mod}(6747^{1223}, 1363)$ , pošto je  $6747 > 1363$ , predstavimo 6747 u bazi od 1363. Dobije se da je  $6747 = 4 \cdot 1363 + 1295$ . Računamo  $D_A$  za 4 i 1295. Dobije se  $D_A(6747) = 444 \cdot 1363 + 240 = 605412$ . Pa je  $E_B(605412) = \text{mod}(605412^{73}, 1271)$ . Uradimo sličan postupak kao i ranije pošto  $605412 > 1271$ . Konačno, dobije se da je digitalni potpis:

$$z = 455 \cdot 1271 + 755 \implies \underline{z = 579060}$$

d)

Bogdan pristupa dešifrovanju poruke  $y = 518640$ .

$$x = D_B(518640) = \text{mod}(518640^{937}, 1271)$$

Pošto  $y > 1271$ , izrazimo  $y$  po bazi 1271. Dobije se  $518640 = 408 \cdot 1271 + 72$ . Računamo cifre posebno:

$$D_B(408) = \text{mod}(408^{937}, 1271) = 5$$

$$D_B(72) = \text{mod}(72^{937}, 1271) = 392$$

Bogdan je dešifrovanjem dobio  $x = 5 \cdot 1271 + 392 \implies \underline{x = 6747}$ . Dobio je izvornu poruku što je i trebao da dobije. Provjeravamo digitalni potpis formulom:

$$E_A(D_B(z)) \rightarrow E_A(D_B(579060))$$

Prvo računamo  $D_B(579060)$ , računa se na isti način kao i prethodni primjeri, svakako mora se svesti na bazu 1271 pa posebno računati cifre. Dobije se da je  $D_B(579060) = 605412$ . Sada računamo  $E_A(605412)$ , također, na veoma sličan način dobijemo da je  $E_A(605412) = 6747$ .

Zaključujemo da je poruka zaista došla od Aide.