Diskretna matematika

Zadaća 1

Vedad Fejzagić

Oktobar 22, 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:

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

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 $k \in Z$ 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:

$$z^* = 54$$
$$k^* = -8 \cdot 54 = -432$$

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

$$z = 54 + t, t \in Z$$

Vraćamo u početnu jednačinu:

$$5x + 11y = 54 - 9(54 + t)$$
$$5x + 11y = -432 - 9t$$

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:

$$x = 864 + 18t + 11s$$
$$y = -432 - 9t - 5s$$
$$z = 54 + t$$
$$t, s \in Z$$
$$\text{uz ograničenja } x, y, z > 0$$

Pristupamo rješavanju sistema nejednačina:

$$x = 864 + 18t + 11s > 0 \tag{1}$$

$$y = -432 - 9t - 5s \implies y = 432 + 9t - 5s < 0 \tag{2}$$

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

Iz (2):

$$s < \frac{-9t - 432}{5} \tag{A}$$

Iz (1):

$$s > \frac{-864 - 18t}{11} \tag{B}$$

Možemo zaključiti:

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

Rješenja za t:

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

tj.

$$t \in [-49, -53], t \in Z$$

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

Za $t = -51$:

$$(A) \implies s < \frac{27}{5}(= 5.4)$$
$$(B) \implies s > \frac{54}{11}(\sim 4.9)$$
$$s \in (\frac{54}{11}, \frac{27}{5})$$

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:

$$NZD(9,10) = 1$$
$$NZD(9,17) = 1$$
$$NZD(10,17) = 1$$

Očigledno je da kinesku teoremu o ostacima možemo primjeniti.

$$n1 \cdot n2 \cdot n3 = 9 \cdot 10 \cdot 17 = 1530$$

$$\lambda 1 = \frac{1530}{9} = 170$$

$$\lambda 2 = \frac{1530}{10} = 153$$

$$\lambda 3 = \frac{1530}{17} = 90$$

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:

$$170x_1 \equiv 8 \pmod 9 \tag{A}$$
$$153x_2 \equiv 2 \pmod{10} \tag{B}$$
$$90x_3 \equiv 0 \pmod{17}$$

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:

$$(A) \rightarrow 170 > 9 \rightarrow mod(170, 9) = 8 \implies 8x_1 \equiv 8 \pmod 9$$
$$(B) \rightarrow 153 > 10 \rightarrow mod(153, 10) = 3 \implies 3x_2 \equiv 2 \pmod{10}$$

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 $0 \leq x < 1530$

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

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

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

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

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:

$$\begin{aligned} 782 &\equiv 8 \pmod 9 \implies 782 + 9y = 8 \implies y \in Z \\ 782 &\equiv 2 \pmod{10} \implies 782 + 10y = 2 \implies y \in Z \\ 782 &\equiv 0 \pmod{17} \implies 782 + 17y = 0 \implies y \in Z \end{aligned}$$

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:

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

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

$$89 = \quad (\text{mod } a \cdot 65 + b, 26) + 65$$
$$71 = \quad (\text{mod } a \cdot 69 + b, 26) + 65$$

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:

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

$NZD(4,26) = 2$, $2 \mid 18$, 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 $y = \pmod{2x + 24, 26} + 65$. Dakle, $2x + 24$ je uvijek paran broj pa je i $\pmod{2x + 24, 26}$ 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:

$$y = \pmod{15x + 11, 26} + 65$$

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':

$$y = \pmod{15x + 11, 26} + 65$$
$$y = \pmod{15(65 + x') + 11, 26} + 65$$
$$y = \pmod{986 + 15x', 26} + 65 \to y = \pmod{15x' + 24, 26} + 65$$

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

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

Pa izrazimo x':

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

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

Pa je opće rješenje za x'

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

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

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

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 dešifiriranja je data ispod:

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

Dešifrovana poruka glasi:

DISKRETNAMATEMATIKANIJETESKANIZAKOGAKOVJEZBAREDOVNO

Ako dodamo razmake:

DISKRETNA MATEMATIKA NIJE TESKA NI ZA KOGA KO VJEZBA REDOVNO

Zadatak 4

a)

$$8x + 10y + 17z \equiv 64 \pmod{93} \tag{1}$$
$$12x + 9y + 19z \equiv 3 \pmod{93} \tag{2}$$
$$7x + 14y + 15z \equiv 68 \pmod{93} \tag{3}$$

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 $744 > 93 \implies mod(744, 93) = 0$, 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, $k \in Z$. 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 promjenjivoj 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:

$$y = 10 + 31t, t \in Z$$

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 $y = 207 + 26t, t \in Z$. 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 $y = 25 + 26t, t \in Z$. Isti izraz vraćamo u prvu kongruenciju tj.

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

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 $x = -5 + 39t, t \in Z$. 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:

$$x \equiv 34 \pmod{39}$$
$$y \equiv 25 \pmod{26}$$

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

$$x = 34, y = 25; x = 34, y = 51; x = 34, y = 77$$
$$x = 73, y = 25; x = 73, y = 51; x = 73, y = 77$$

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:

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

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

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

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 $mod(1033, 8) = 1$. Ispitajmo ostale uvjete:

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

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

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:

$$(79 \mid 3) = (mod(79, 3) \mid 3) = (1 \mid 3) = 1$$
$$(79 \mid 5) = (mod(79, 5) \mid 5) = (4 \mid 5) = (2^2 \mid 5) = 1$$

Međutim, dopunski uvjet nije zadovoljen jer $mod(79, 8) = 7 \neq 1$. 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:

$$(15|7) = (mod(15, 7)|7) = (1|7) = 1$$
$$(15|11) = (mod(15, 11)|11) = (4|11) = (2^2|11) = 1$$

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)

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

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

Probajmo za $\underline{g = 2}$

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

Uvjet nije zadovoljen, probajmo sa $\underline{g = 3}$

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

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

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

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

$t = 0 \to x = 30$ 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:

$$x = mod(64^6, 89) = 8$$
$$x = 89 - 8 = 81$$

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:

$$mod(37, 4) \neq 3$$
$$mod(37, 8) = 5$$

Pa je jedno tipično rješenje:

$$x = mod(a^{\frac{p+3}{8}} \cdot 2^{\frac{p-1}{4}}, p)$$
$$x = mod(11^5 \cdot 2^9, 37)$$
$$x = 23 (= x_1)$$

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

$$[h]_p = ([2 \cdot x1]_p)^{-1} = ([46]_{37})^{-1}$$

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

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

$$x_2 = mod(x_1 - h((x_1)^2 - a), p^2)$$
$$x_2 = mod(23 - 33(23^2 - 85), 37^2)$$
$$x_2 = 939$$

Zaključujemo da su rješenja:

$$x = 939$$
$$x = 1369 - 939 = 430$$

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:

$$x^2 \equiv 9 \pmod 7$$
$$x^2 \equiv 9 \pmod{19}$$

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

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

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

$$x = 16$$
$$x = 3$$

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

$$x \equiv 4 \pmod 7, x \equiv 16 \pmod{19} \tag{1}$$
$$x \equiv 3 \pmod 7, x \equiv 16 \pmod{19} \tag{2}$$
$$x \equiv 4 \pmod 7, x \equiv 3 \pmod{19} \tag{3}$$
$$x \equiv 3 \pmod 7, x \equiv 3 \pmod{19} \tag{4}$$

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:

$$n_1 \cdot n_2 = 133$$
$$\lambda_1 = \frac{133}{7} = 19$$
$$\lambda_2 = \frac{133}{19} = 7$$
$$x = 19x_1 + 7x_2 \pmod{133}$$

<u>Rješavamo prvi sistem:</u>

$$19x_1 \equiv 4 \pmod 7$$
$$7x_2 \equiv 16 \pmod{19}$$

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:

$$x_1 = 12 + 7t, t \in Z \to t = -1 \to \underline{x_1 = 5}$$
$$x_2 = -128 + 19t, t \in Z \to t = 7 \to \underline{x_2 = 5}$$

Na kraju, rješenje prvog sistema je:

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

Rješavamo drugi sistem:

$$19x_1 \equiv 3 \pmod{7}$$
$$7x_2 \equiv 16 \pmod{19}$$

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

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

Rješenje drugog sistema je:

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

Rješavamo treći sistem:

$$19x_1 \equiv 4 \pmod 7$$
$$7x_2 \equiv 3 \pmod{19}$$

Prva kongruencija je rješena ranije $\underline{x_1 = 5}$, diofantova jednačina je ista kao i tokom rješavanja prvog sistema. Dakle:

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

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 rješene 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. $z = 3710 + 209t, t \in Z$. 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:

$$n_1 \cdot n_2 = 209$$
$$\lambda_1 = \frac{209}{11} = 19$$

$$\lambda_2 = \frac{209}{19} = 11$$
$$y = 19y_1 + 11y_2 \pmod{209}$$

<u>Rješavamo prvi sistem:</u>

$$19y_1 \equiv 5 \pmod{11}$$
$$11y_2 \equiv 9 \pmod{19}$$

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:

$$y_1 = -20 + 11t, t \in Z \to t = 2 \to \underline{y_1 = 2}$$
$$y_2 = 63 + 19t, t \in Z \to t = -3 \to \underline{y_2 = 6}$$

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 rješena u prethodnom slučaju, $\underline{y_2 = 6}$. Odgovarajuća diofantova jednačina je ista kao i u prethodnom slučaju. Lahko zaključujemo da vrijedi:

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

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 rješena ranije $\underline{y_1 = 2}$, diofantova jednačina je ista kao i tokom rješavanja prvog sistema. Dakle:

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

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:

$$x = 936 + 1881t, t \in Z$$
$$x = 252 + 1881t, t \in Z$$
$$x = 1629 + 1881t, t \in Z$$
$$x = 945 + 1881t, t \in Z$$

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:

$$x = 252$$
$$x = 936$$
$$x = 945$$
$$x = 1629$$
$$x = 2133$$
$$x = 2817$$
$$x = 2826$$
$$x = 3510$$
$$x = 4014$$
$$x = 4698$$
$$x = 4707$$
$$x = 5391$$