# Zadaća 1

## iz predmeta Diskretna matematika

Prezime i ime: Hamzić Huso

Broj indeksa: 18305

Grupa: DM2 [Pon 15.00]

Odgovorni demonstrator: Šeila Bećirović

| Zadatak | Bodovi |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | |
| 8 | |

Elektrotehnički fakultet Sarajevo

*PAŽNJA! : U dokumentu neke sporedne računice koje su trivijalne su preskočene (npr računanje NZD-a koje je provedeno na papiru i ostale sitnice) samo zato kako ne bih gubio vrijeme na stvari koje nisu u fokusu prilikom izrade ovih zadataka i koje ni na ispitu ne bi bile u fokusu, po ugledu na rješenja naših tutorijala i ZSR-ova.*

1. Za potrebe neke vitaminske terapije koriste se tri vrste tableta $T_1$, $T_2$ i $T_3$ koje respektivno sadrže 15, 33, odnosno 18 jedinica nekog vitamina. Terapijom je potrebno unijeti 132 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.

*Neka su x, y i z respektivno brojevi tableta $T_1$, $T_2$ i $T_3$. Očito je da se problem svodi na ekvivalentnu Diofantovu jednačinu:*

***15x + 33y + 18z = 132***

*Rješenja ćemo tražiti u skupu pozitivnih cijelih brojeva, obzirom da tablete nije dozvoljeno lomiti ($x \geq 0, y \geq 0, z \geq 0$).*

*Provjerimo rješivost jednačine u skupu cijelih brojeva ($\mathbb{Z}$),*
*tako što ćemo naći **NZD** (15, 33, 18):*
*Ovaj problem možemo pogodno računski predstaviti kao **NZD** (**NZD**(15, 33), 18)[1].*
*Najprije ćemo naći **NZD** (15, 33):*
*Očigledno je da je **NZD** (15, 33) = 3.*

*Dobijeni izraz vratimo u [1] pa imamo:*
**NZD** (15, 33, 18) = **NZD** (3, 18)
*Obzirom da $18 = 6 \cdot 3$, vrijedi:* **NZD** (15, 33, 18) = 3.
*Jednačina je stoga rješiva u skupu $\mathbb{Z}$ jer **NZD** (15, 33, 18) = 3 te vrijedi 3|132.*

*Nakon dijeljenja sa 3 dobijamo ekvivalentnu jednačinu **5x + 11y + 6z = 44**, sada pristupamo njenom rješavanju:*
*Napišimo jednačinu u obliku **5x + 11y = 44 - 6z**. Kako je **NZD** (5, 11) = 1, a 1 dijeli svaki cijeli broj, rješenja date jednačine za x i y će postojati za svako z.*
*Stoga rješavanjem ove Diofantove po z dobijamo da je $z = 44 + t$, pa jednačina glasi*

***5x + 11y = 44 - 6(44 + t)**.*

*Lako možemo naći rastavu $1 = -2 \cdot 5 + 1 \cdot 11$, pa opće rješenje možemo izraziti kao:*

$$x = -2 \cdot (-220 - 6t) + 11s = 440 + 12t + 11s$$
$$y = 1 \cdot (-220 - 6t) - 5s = -220 - 6t - 5s$$
$$z = 44 + t$$

*pri čemu su s i t proizvoljni cijeli brojevi iz $\mathbb{Z}$ ($s \in \mathbb{Z}$, $t \in \mathbb{Z}$).*
*Sada tražimo one vrijednosti s i t za koje vrijede dopunska ograničenja iz postavke zadatka ($x \geq 0, y \geq 0, z \geq 0$):*

$$440 + 12t + 11s \geq 0 \rightarrow s \geq -40 - \frac{12t}{11}$$
$$-220 - 6t - 5s \geq 0 \rightarrow s \leq -220 - \frac{6t}{5}$$
$$t \geq -44$$

*Odnosno možemo pisati:*

$-40 - \frac{12t}{11} \leq s \leq -220 - \frac{6t}{5} \rightarrow -40 - \frac{12t}{11} \leq -220 - \frac{6t}{5}$

*Kada sve sredimo i prebacimo nepoznate na jednu stranu dobijamo:*

$6t \leq -220 \rightarrow t \leq (\sim -36.66)$

*Sada je potrebno ispitati sve slučajeve za* $-44 \leq t \leq -37$*:*

**1. za t = -44:** *Kada sve sredimo i prebacimo nepoznate na jednu stranu dobijamo:*

$8 \leq s \leq 8.8$

**Izraz je zadovoljiv samo za s = 8.**

**I zaista, za t = -44 i s = 8** :

x = 0, y = 4, z = 0

$33 \cdot 4 = 132$

$132 = 132$

**Prvo rješenje naše jednačine je** $\boxed{(x_1, y_1, z_1) = (0, 4, 0).}$

**2. za t = -43:** $\sim 6.9 \leq s \leq \sim 7.6$

**Izraz je zadovoljiv samo za s = 7.**

**I zaista, za t = -43 i s = 7** :

x = 1, y = 3, z = 1

$15 \cdot 1 + 33 \cdot 3 + 18 \cdot 1 = 132$

$132 = 132$

**Drugo rješenje naše jednačine je** $\boxed{(x_2, y_2, z_2) = (1, 3, 1).}$

**3. za t = -42:** $\sim 5.81 \leq s \leq \sim 6.4$

**Izraz je zadovoljiv samo za s = 6.**

**I zaista, za t = -42 i s = 6** :

x = 2, y = 2, z = 2

$15 \cdot 2 + 33 \cdot 2 + 18 \cdot 2 = 132$

$132 = 132$

**Treće rješenje naše jednačine je** $\boxed{(x_3, y_3, z_3) = (2, 2, 2).}$

**4. za t = -41:** $\sim 4.72 \leq s \leq \sim 5.2$

**Izraz je zadovoljiv samo za s = 5.**

**I zaista, za t = -41 i s = 5** :

x = 3, y = 1, z = 3

$15 \cdot 3 + 33 \cdot 1 + 18 \cdot 3 = 132$

$132 = 132$

**Četvrto rješenje naše jednačine je** $\boxed{(x_3, y_3, z_3) = (3, 1, 3).}$

**5. za t = -40:** $\sim 3.63 \leq s \leq \sim 4$

**Izraz je zadovoljiv samo za s = 4.**

**I zaista, za t = -40 i s = 4** :

x = 4, y = 0, z = 4

$15 \cdot 4 + 18 \cdot 4 = 132$

$132 = 132$

**Peto rješenje naše jednačine je** $\boxed{(x_4,\, y_4,\, z_4) = (4,\, 0,\, 4).}$

**6. za t = -39:** $\sim 2.54 \leq s \leq 2.8$
**Izraz nije zadovoljiv niti za jedno $s \in \mathbb{Z}$, pa jednačina za t = -39 nema rješenja.**
**7. za t = -38:** $\sim 1.45 \leq s \leq 1.6$
**Izraz nije zadovoljiv niti za jedno $s \in \mathbb{Z}$, pa jednačina za t = -38 nema rješenja.**
**8. za t = -37:** $\sim 0.36 \leq s \leq 0.4$
**Izraz nije zadovoljiv niti za jedno $s \in \mathbb{Z}$, pa jednačina za t = -37 nema rješenja.**

*Dobili smo pet načina na koje se može realizirati terapija koristeći tablete $T_1$, $T_2$ i $T_3$. Da bismo postigli unos od 132 jedinica vitamina možemo koristiti:*

- **4 tablete $T_2$**
- **1 tabletu $T_1$, 3 tablete $T_2$ i 1 tabletu $T_3$**
- **2 tablete $T_1$, 2 tablete $T_2$ i 2 tablete $T_3$**
- **3 tablete $T_1$, 1 tabletu $T_2$ i 3 tablete $T_3$**
- **4 tablete $T_1$ i 4 tablete $T_3$**

2. Čopor majmuna je skupljao banane. Kada su skupljene banane pokušali razmjestiti u 13 jednakih gomila, ispostavilo se da preostaje 11 banana koje je nemoguće rasporediti tako da gomile budu jednake. Slično, kada su probali rasporediti banane u 21 jednakih gomila, preostale su 2 banane. Međutim, uspjeli su skupljene banane razmjestiti u 22 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 očito svodi na rješavanje sistema kongruencija:*

$$x \equiv 11 \ (mod\ 13)$$
$$x \equiv 2 \ (mod\ 21)$$
$$x \equiv 0 \ (mod\ 22).$$

*Krenimo sa rješavanjem ovog sistema metodom Kineske teoreme o ostacima:*
*Mora vrijediti **NZD** (11, 13) = 1, što se lako i pokaže obzirom da su 11 i 13 prosti brojevi, također mora i vrijediti **NZD** (2, 21)=1 kao i **NZD** (0, 22)=1 što očito vrijedi jer je 21 prost broj a 0 je uzajamno prosta sa svakim drugim brojem. Imamo:*

$$\lambda_1 = \frac{13 \cdot 21 \cdot 22}{13} = 462$$

$$\lambda_2 = \frac{13 \cdot 21 \cdot 22}{21} = 286$$

$$\lambda_3 = \frac{13 \cdot 21 \cdot 22}{22} = 273$$

*Opće rješenje se može predstaviti u obliku:*
$x \equiv \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 \ (mod\ 13 \cdot 21 \cdot 22) \rightarrow x \equiv 462x_1 + 286x_2 + 273x_3 \ (mod\ 6006)$, *gdje su* $x_1$, $x_2$ *i* $x_3$ *bilo koja rješenja kongruencija*
$462x_1 \equiv 11 \ (mod\ 13)$, $286x_2 \equiv 2 \ (mod\ 21)$ *i* $273x_3 \equiv 0 \ (mod\ 22)$.

*Pristupimo rješavanju ovih kongruencija*
*Prva kongruencija je analogna Diofantovoj jednačini* $\boldsymbol{462x_1 + 13y = 11}$.
***NZD** (462, 13)=1 pa je jednačina rješiva a rastava glasi:* $1 = 2 \cdot 462 - 71 \cdot 13$, *pa je opće rješenje za* $x_1$*:*
$x_1 = 2 \cdot 11 + 13t \rightarrow \boxed{\boldsymbol{x = 22 + 13t}}$
*Ovo možemo kraće zapisati kao* $x \equiv 9 \ (mod\ 13)$

*Driga kongruencija je analogna Diofantovoj jednačini* $\boldsymbol{286x_2 + 21y = 2}$.
***NZD** (286, 21)=1 pa je jednačina rješiva a rastava glasi:* $1 = -8 \cdot 286 + 109 \cdot 21$, *pa je opće rješenje za* $x_2$*:*
$x_2 = -8 \cdot 2 + 21t \rightarrow \boxed{\boldsymbol{x = -16 + 21t}}$
*Ovo možemo kraće zapisati kao* $x \equiv 5 \ (mod\ 21)$

*Rješenje treće kongruencije je očigledno* $\boxed{\boldsymbol{x = 0 + 22t}}$.

*Ukoliko uzmemo tipična rješenja:* $x_1 = 9, x_2 = 5$ *i* $x_3 = 0$, *opće rješenje možemo izraziti u obliku:*
$x \equiv 462 \cdot 9 + 286 \cdot 5 + 0 \ (mod\ 6006) \rightarrow 5588 \ (mod\ 6006)$
*Ovo je opće rješenje sistema kongruencija, možemo ga izraziti i kao*
$x = 5588 + 6006t \ (t \in \mathbb{Z})$.
*Jasno je da će ovo rješenje imati minimalnu vrijednost za* $t = 0$, *pa je stoga najmanji broj banana za koji je scenario iz zadatka mogući,* ***5588 banana.***

3. 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

   VWYMDQTXKCKTQCKTWMKXWRQTQYMKXWPKMSGKMSJRQPFKDQVSJXS

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

   - Izvorna poruka je u cijelosti pisana bosanskim jezikom, isključivo velikim slovima unutar engleskog alfabeta (ASCII kodovi u opsegu od 65 do 91);
   - Za šifriranje je korišten algoritam prema kojem se svaki znak izvorne poruke čiji je ASCII kod x mijenja znakom sa ASCII kodom y prema formuli y = 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:

- 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;
- Odredite funkciju dešifriranja, tj. funkciju kojom se vrši rekonstrukcija x iz poznatog y;
- 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).

*Najprije trebamo postaviti početne kongruencije. Znamo da se u bosanskom jeziku slovo 'A' ponavlja najviše puta, pa je za očekivati da u kodiranom stringu slovo sa najviše ponavljanja odgovara slovu 'A'.*

*Nije teško provjeriti da je to slovo K koje se ponavlja 8 puta. ASCII kod slova 'A' je 65, a slova 'K' je 75.*

*Stoga imamo našu prvu kongruenciju:*

$65a + b + 65 \equiv 75 (mod\ 26)$, *odnosno* $65a + b \equiv 10\ (mod\ 26)$

*Drugu kongruenciju dobijamo iz uvjeta da je drugo najčešće slovo slovo 'E'. Analogno se pokaže da u kodiranom stringu najviše ponavljanja također ima slovo 'Q' koje se ponavlja 6 puta.*

*ASCII kod 'Q' je 81 pa time dobijamo i drugu kongruenciju:*

$69a + b + 65 \equiv 81\ (mod\ 26)$, *odnosno* $69a + b \equiv 16\ (mod\ 26)$

*Ako oduzmemo prvu od druge kongruencije imamo:*

$4a \equiv 6\ (mod\ 26)$

*Očigledno je NZD (4, 26) = 2 i vrijedi 2|20, pa kongruenciju dijelimo sa 2. Imamo:*

$2a \equiv 3\ (mod\ 13)$. *Rastavu pišemo kao:*

$1 = -6 \cdot 2 + 1 \cdot 13$, *pa je opće rješenje za a:*

$a \equiv -18\ (mod\ 13)$, *odnosno* $\boxed{a \equiv 8\ (mod\ 13)}$

*Drugo tipično rješenje pored a = 8 je a = 21.Uvrstimo li u drugu kongruenciju tipično rješenje a = 21. Imamo:*

$1365 + b \equiv 10\ (mod\ 26)$, *odnosno* $b \equiv -1355\ (mod\ 26) \rightarrow \boxed{b \equiv 23\ (mod\ 26)}$

*Konstante a i b su tipična rješenja svojih kongruencija, a = 21 i b = 23.*

*Funkcija dešifriranja iz poznatog x time glasi:*

$\boxed{((21x + 23)\ mod\ 26) + 65}$

*Dešifrovani string glasi:*

***DISKRETNAMATEMATIKANIJETESKANIZAKOGAKOVJEZBAREDOVNO***

*Za dešifrovanje je korištena jednostavna C++ funkcija:*

```
        void desifruj(string &sifra)
{
    int j=0;
    for(int i=65; i<=91; i++)
    {
        if((21*i+23)%26 + 65==sifra[j])
        {
            std::cout<<(char)i<<" ";
            i=64;
            j++;
            continue;
        }
    }

}
```

4. Riješite sljedeće sisteme linearnih kongruencija i izdvojite im tipična rješenja:

a)$7x + 10y + 15z \equiv 43 \ (mod\ 87), 9x + 3y + 15z \equiv 18 \ (mod\ 87), 18x + 14y + 9z \equiv 61 \ (mod\ 87)$
b) $21x + 9y \equiv 12 \ (mod\ 30), 10x + 16y \equiv 4 \ (mod\ 30)$

*a) Najprije pomnožimo prvu kongruenciju sa -1 i treću sa -5, što je regularno jer su* ***NZD*** *(87, -1)=1 i* ***NZD*** *(-5, 87)=1 Imamo:*

$$-7x - 10y - 15z \equiv -43 \ (mod\ 87)$$
$$9x + 3y + 15z \equiv 18 \ (mod\ 87)$$
$$-90x - 70y - 45z \equiv -305 \ (mod\ 87)$$

*Sada drugu kongruenciju dodajmo na prvu te je također pomnožimo sa 3 i dodajmo na treću. Imamo:*

$$2x - 7y \equiv -25 \ (mod\ 87)$$
$$9x + 3y + 15z \equiv 18 \ (mod\ 87)$$
$$-63x - 61y \equiv -251 \ (mod\ 87)$$

*Sada treću kongruenciju pomnožimo sa 2 što je regularno jer je* ***NZD*** *(87, 2)=1 te na nju dodajmo prvu kongruenciju pomnoženu sa 63. Imamo:*

$$2x - 7y \equiv -25 \ (mod\ 87)$$
$$9x + 3y + 15z \equiv 18 \ (mod\ 87)$$
$$46y \equiv -2077 \ (mod\ 87)$$

*Izvršimo redukciju po modulu treće kongruencije. Imamo*

$$2x - 7y \equiv -25 \ (mod\ 87)$$
$$9x + 3y + 15z \equiv 18 \ (mod\ 87)$$
$$46y \equiv 11 \ (mod\ 87)$$

*Riješimo treću kongruenciju:*
*Ona se svede na Diofantovu jednačinu: 46y + 87k = 11*

***NZD** (46, 87)=1 a 1 dijeli 11, pa imamo rastavu primjenom proširenog Euklidovog algoritma:*

$$1 = (-17) \cdot 46 + 9 \cdot 87$$

*Odakle slijedi da je rješenje:* $y \equiv -187 \pmod{87}$

*odnosno, kada reduciramo po modulu 87 imamo:* $\boxed{y \equiv 74 \pmod{87}}$

*Preostaju nam prve dvije kongruencije:*

$$2x - 7y \equiv -25 \pmod{87}$$
$$9x + 3y + 15z \equiv 18 \pmod{87}$$

*Uvrštavanjem rješenja za y u prvu kongruenciju te je sređujući dobijamo novu kongruenciju:*

$$2x \equiv 493 \pmod{87}$$

*Redukcijom po modulu 87 imamo:*

$$2x \equiv 58 \pmod{87}$$

*Sada dobijamo Diofantovu jednačinu koja glasi:*

$$2x + 87y = 58$$

*Kako je **NZD** (2, 87) = 1 te kako 1/44 imamo rastavu:* $1 = (-43) \cdot 2 + 1 \cdot 87$

*Odakle slijedi nakon redukcije po modulu 87 da je:*

$$\boxed{x \equiv 29 \pmod{87}}$$

*Sada kada imamo rješenja x = 74 i y = 29, uvrstimo ih u drugu početnu kongruenciju te je sredimo. Imamo:*

$$z \equiv -930 \pmod{87}$$

*Naravno redukcijom po modulu 87 slijedi da je*

$$\boxed{z \equiv 27 \pmod{87}}$$

*Uvrštavanjem dobivenih rješenja* $\boldsymbol{x = 29}$, $\boldsymbol{y = 74}$ *i* $\boldsymbol{z = 27}$ *u početne kongruencije, vidimo da su sve tri zadovoljene što implicira da su rješenja tačna.*

*b) Najprije pomnožimo drugu kongruenciju sa -1 i dodajmo na prvu. Imamo:*

$$11x - 7y \equiv 8 \pmod{30}$$
$$10x + 16y \equiv 4 \pmod{30}$$

*Sada pomnožimo prvu kongruenciju također sa -1 i dodajmo na drugu. Imamo:*

$$11x - 7y \equiv 8 \pmod{30}$$
$$-x + 23y \equiv -4 \pmod{30}$$

*Pomnožimo drugu kongruenciju sa 11 i dodajmo na prvu. Imamo:*

$$246y \equiv -36 \pmod{30}$$
$$-x + 23y \equiv -4 \pmod{30}$$

*Reducirajmo prvu kongruenciju po modulu 30. Imamo*

$$6y \equiv 24 \pmod{30}$$
$$-x + 23y \equiv -4 \pmod{30}$$

*Riješimo prvu kongruenciju.Dobijamo Diofantovu jednačinu:*

$$6y + 30z = 24$$

*Kako je* ***NZD*** *(6, 30) = 6 a 6|24 to je ova Diofantova jednačina rješiva. Podijelimo jednačinu sa 6. Imamo:*

$$y + 5z = 4 \rightarrow \textbf{NZD}(1,\ 5) = 1 \text{ a } 1|4$$

*Pa imamo rastavu:*

$$1 = 6 \cdot 1 - 1 \cdot 5$$

*Odakle slijedi* $\rightarrow y \equiv 6 \cdot 4\ (mod\ 5)$ *odnosno* $\boxed{y \equiv 24\ (mod\ 5)}$

*odnosno* $y = 4 + 5t$*, odakle imamo tipična rješenja:*

$$y_0 = 4$$
$$y_1 = 9$$
$$y_2 = 14$$
$$y_3 = 19$$
$$y_4 = 24$$
$$y_5 = 29$$

*Sada kada vratimo jedno po jedno rješenje za y u drugu kongruenciju dobijamo redom kongruencije:*

$$x_0 \equiv 96\ (mod\ 30)$$
$$x_1 \equiv 211\ (mod\ 30)$$
$$x_2 \equiv 326\ (mod\ 30)$$
$$x_3 \equiv 441\ (mod\ 30)$$
$$x_4 \equiv 556\ (mod\ 30)$$
$$x_5 \equiv 671\ (mod\ 30)$$

*odnosno dobijamo sljedeće uređene parove za rješenje sistema:*

$$\boxed{x_0 = 6\ i\ y_0 = 4}$$
$$\boxed{x_1 = 1\ i\ y_1 = 9}$$
$$\boxed{x_2 = 26\ i\ y_2 = 14}$$
$$\boxed{x_3 = 21\ i\ y_3 = 19}$$
$$\boxed{x_4 = 16\ i\ y_4 = 24}$$
$$\boxed{x_5 = 11\ i\ y_5 = 29}$$

*Uvrštavajući ova rješenja u početne kongruencije možemo viditi da ih rješenja zadovoljavaju.*

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

   - $x^2 \equiv 471\ (mod\ 1235)$
   - $x^2 \equiv 929\ (mod\ 2200)$
   - $x^2 \equiv 375\ (mod\ 748)$
   - $x^2 \equiv 225\ (mod\ 63525)$

*a) Najprije provjerimo da li je kongruencija* $x^2 \equiv 471\ (mod\ 1235)$ *rješiva:*

*Obzirom da je 1235 =* $5 \cdot 13 \cdot 19$*, da bi kongruencija bila rješiva mora zadovoljavati:*
*(471 | 5) = 1, (471 | 13) = 1 i (471 | 19) = 1:*
*(471 | 5) = (471 mod 5 | 5) = (1 | 5) = 1 pa je prvi uvjet zadovoljen.*
*(471 | 13) = (471 mod 13 | 13) = (3 | 13) = (13 | 3)·*$(-1)^{\frac{12\cdot 2}{4}}$ *= (13 | 3) = (*$13\ mod 3$*, 3) = (1 | 3) = 1, pa je i drugi uslov zadovoljen*
*(471 | 19) = (471 mod 19 | 19) = (15 | 19) = (19 | 15)·*$(-1)^{\frac{18\cdot 14}{4}}$ *= -(19 | 15) = -(*$19\ mod 15$*, 15) = -(4 | 15) = -(*$2^2$ *| 15) = -1, kako treći uslov nije ispunjen to znači da početna kongruencija nije rješiva.*

*b) Najprije provjerimo da li je kongruencija* $x^2 \equiv 929\ (mod\ 2200)$ *rješiva:*
*Obzirom da je 2200 =* $2^3 \cdot 5^2 \cdot 1$*, da bi kongruencija bila rješiva mora zadovoljavati (929 | 5), (929 | 11) i* $mod(929,\ 8) = 1$*(jer je e = 3) a ovo zadnje je zadovoljeno pa preostaje samo još da provjerimo:*
*(929 | 5) = (*$929\ mod\ 5$*, 5) = (4 | 5) = 1 pa je prvi uvjet zadovoljen.*
*(929 | 11) = (*$929\ mod\ 11$*, 11) = (5 | 11) = (11 | 5)·*$(-1)^{\frac{10\cdot 4}{4}}$ *= (11 | 5) = (mod(11, 5) | 11) = (1 | 11) = 1, pa je i drugi uvjet zadovoljen što znači da je kongruencija rješiva.*
*Nećemo ju rješavati ali ćemo odrediti broj rješenja.*
*Kako je* $2200 = 2^3 \cdot 5^2 \cdot 1$ *imamo da je* $k = 2$ *te kako je* $e \geq 3$ *Broj rješenja ove kongruencije je jednak* $2^k \cdot 2^2 \to 2^4 =$ ***16***

*c)Najprije provjerimo da li je kongruencija* $x^2 \equiv 375\ (mod\ 748)$ *rješiva:*
*Obzirom da je 748 =* $2^2 \cdot 11 \cdot 17$*, da bi kongruencija bila rješiva mora zadovoljavati (375 | 11)=1, (375 | 17)=1 i* $mod(375,\ 4) = 1$*(jer je e = 2) a ovo zadnje nije zadovoljeno jer je* $mod(375,\ 4) = 3 \neq 1$ *pa odmah zaključujemo da početna kongruencija nije rješiva*

*d) Najprije provjerimo da li je kongruencija* $x^2 \equiv 225\ (mod\ 63525)$ *rješiva:*
***NZD*** *(225, 63525) = 75* $\neq 1$*, pa je uslov rješivosti da vrijedi* ***NZD*** *(a/q^2, m/d) = 1.*
*Najprije trebamo naći d = p·*$q^2$ *= 75, gdje u rastavi broja p nema nijedan prosti faktor sa eksponentom većim od 1.*
*Možemo pisati p = 3, q = 5* $\to q^2 = 5^2$*, pa je uslov rješivosti* ***NZD*** $(\frac{225}{75},\ \frac{63525}{75}) = 1$*.*
*Imamo:*
***NZD*** *(3, 847) = 1, pa je kongruencija sigurno rješiva.*
*Broj tipičnih rješenja ove kongruencije je n·q, gdje je n broj tipičnih rješenja kongruencije* $y^2 \equiv z_0\ (mod\ 847)$ *gdje je* $z_0$ *tipično rješenje kongruencije* $pz \equiv 3\ (mod\ 847)$
*odnosno* $3z \equiv 3\ (mod\ 847)$
*a ova kongruencija se svodi na Diofantovu jednačinu koju već znamo kako se rješava iz prethodnih zadataka pa ćemo samo napisati rastavu broja:*
$$1 = (-282) \cdot 3 + 1 \cdot 847$$
*odakle dobijamo da je* $z_0 \equiv -282 \cdot 3\ (mod\ 847)$
*odnosno nakon redukcije po modulu 847 imamo* $z_0 \equiv 1\ (mod\ 847)$

*Sada uvrstimo* $z_0$ *u kongruenciju po y i imamo:*
$y^2 \equiv 1\ (mod\ 847)$
*pa sada moramo riješiti ovu kongruenciju.*
*Kako je* $847 = 2^0 \cdot 7 \cdot 11^2$ *dobijamo da moramo riješiti sljedeće kongruencije:*
*1.1)* $y^2 \equiv 1\ (mod\ 7)$ *i 1.2)* $y^2 \equiv 1\ (mod\ 11)$

*a kako su za obje ove kongruencije očita rješenja $y_1 = 1$ i $y_2 = 1$ tako dobijamo i preostala dva kao $m - x$ gdje je m respektivno 7 pa 11*
*tako dobijamo da rješenja kongruencije $y^2 \equiv 1 \pmod{847}$ ima 4 i to:*
$y_1 = \mathbf{1}$, $y_2 = \mathbf{1}$, $y_3 = \mathbf{6}$, $y_4 = \mathbf{10}$

*Svakome od ova 4 tipična rješenja odgovara q tipičnih rješenja polazne kongruencije pa kako imamo 4 tipična rješenja za y to je $\boldsymbol{n = 4}$ dok je ukupan broj rješenja polazne kongruencije jednak $\boldsymbol{n \cdot q}$, tako je broj rješenja jedan* ***20***

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

*a)* $[82]_{113}$
*b)* $[747]_{1369}$
*c)* $[34]_{417}$
*d)* $[1836]_{4185}$

*a) Tražimo x koji je rješenje kongruencije $x^2 \equiv 82 \pmod{113}$, a za koji vrijedi $0 \leq x < 73$.*
***NZD** (82, 113) = 1.*
*Pretpostavimo da je kongruencija rješiva, u suprotnom ćemo zapeti pri rješavanju odnosno dobit ćemo kontradikciju.*
*Kako je p = 113 → prost broj te uočavamo da nije moguće koristiti Lagrangeovu kao ni Legendreovu formulu jer je mod (82, 4) ≠ 3 kao i mod (82, 8) ≠ 5*
*Koristit ćemo Tonellijev algoritam, koji prvo traži da odaberemo **g** tako da je (g | 113) = -1*
*Uzmimo g = 3 jer (3 |113) = -1, što se lako i pokaže.*
*Sada nađimo inv (3, 113):*
*napišimo ovo u modularnoj aritmetici i imamo:*
$h = ([3]_{113})^{-1}$ *kako je **NZD** (3, 113) = 1 tako primjenom Fermat-Eulerove teoreme ovo možemo napisati kao* $([3]_{113})^{112-1}$ *pri čemu je 112 iznos Eulerove totientne funkcije za* $m = 113$ *jer je 113 prost broj*
*odnosno lahko primjenjujući algoritam kvadriraj i množi dobijamo da je*
$h = ([3]_{113})^{111} = [38]_{113}$ *odnosno* $\boldsymbol{h = 38}$
*Implementirao sam Tonellijev algoritam kao c++ kod:*

```
    void Tonelli()
{
    int t=113/2, v=1, w=82, h=38;
    int x=0;
        while(t%2==0)
        {
            t=t/2; h = (h*h)%113;
            if(std::pow(w, t)%p!=1)
            {
                v=(v*g)%113; w=(w*h)%113;
            }
            g=(g*g)%113;
        }
        x=(v * std::pow(w, (t+1)/2))%113;
        std::cout<<x;

}
```

*Odakle dobijamo da je* $\boxed{x \equiv 46 \ (mod\ 113)}$ *i* $\boxed{x \equiv 67 \ (mod\ 113)}$

*Provjerom lahko utvrđujemo da su rješenja kongruencije ispravna te da je kongruencija rješiva to jest da nismo dobili nikakvu kontradikciju.*

*b) Tražimo x koji je rješenje kongruencije* $x^2 \equiv 747 \ (mod\ 1369)$*, a za koji vrijedi* $0 \leq x < 1369$.

***NZD** (747, 1369) = 1, pa treba provjeriti rješivost.*
*Korisno je primijetiti da je modul u obliku* $m = p^k$ *odnosno 1369 =* $37^2$

*Sada je potrebno naći jedno tipično rješenje kongruencije* $x_1 \equiv 747 \ (mod\ 37)$ *kako bi mogli primjeniti Henselovu formulu.*
*Redukcijom pomoćne kongruencije po modulu 37 dobijamo:*
$x_1 \equiv 7 \ (mod\ 37)$
*Sada kako je 37 prost broj, te kako vrijedi mod(37, 8) = 5 možemo primjeniti Legendreovu formulu* $x_1 = mod(a^{\frac{p+3}{8}}, p)$ *, odnosno* $x_1 = mod(7^{\frac{37+3}{8}}, 37)$

$\boxed{x_1 = 9}$ *te uočimo da* $x_1$ *zadovoljava kongruenciju.*

*Sada računamo* $[h]_p = ([2 \cdot x_1]_p)^{-1}$ *po Henselovoj formuli, odnosno* $[h]_{37} = ([18]_{37})^{-1}$
*Kako je 37 prost broj te kako je **NZD** (18, 37) = 1, možemo primjeniti Euler-Fermatovu teoremu za nalaženje inverznog elementa za množenje te uz primjenu kvadriraj i množi dobijamo da je* $\boxed{h = 35}$

*Sada kako je* $e = 2 \rightarrow x_e$ *odnosno*
$x = mod(x_1 - h(x_1^2 - a), p^2)$
*Kada uvrstimo da je* $x_1 = 9$, $h = 35$ *i* $p = 37$ *dobijamo da je:*

$\boxed{x = 46}$ *prvo tipično rješenje kongruencije, a drugo dobijamo kao m -* $x_e$

*odnosno x = 1369 - 46 →* $\boxed{x = 1323}$ *uvrštavajući ova rješenja u početnu kongruenciju vidimo da je ona zadovoljena.*

*c) Tražimo x koji je rješenje kongruencije* $x^2 \equiv 34 \pmod{417}$*, a za koji vrijedi* $0 \leq x < 417$.
***NZD** (34, 417) = 1*
*Primjetimo da je* $417 = 3 \cdot 139$
*Pristupimo rješavanju pomoćnih kongruencija:*
$x^2 \equiv 34 \pmod 3$ *i* $x^2 \equiv 34 \pmod{139}$

*Redukcijom po modulu 3 prve kongruencije dobijamo kongruenciju* $x^2 \equiv 1 \pmod 3$
*odakle vidimo da je jedno očito rješenje* $\boldsymbol{x = 1}$ *dok je drugo x = 3 - 1 odnosno* $\boldsymbol{x = 2}$

*kod kongruencije* $x^2 \equiv 34 \pmod{139}$ *primjetimo da vrijedi mod(139, 4) = 3 pa možemo primjeniti Lagrangeovu formulu odakle dobijamo rješenja* $\boldsymbol{x = 112}$ *i* $\boldsymbol{x = 27}$

*Možemo izvući četiri sistema kongruencija:*
$x \equiv 1 \pmod 3$ *i* $x \equiv 112 \pmod{139}$
$x \equiv 1 \pmod 3$ *i* $x \equiv 27 \pmod{139}$
$x \equiv 2 \pmod 3$ *i* $x \equiv 112 \pmod{139}$
$x \equiv 2 \pmod 3$ *i* $x \equiv 27 \pmod{139}$

*Sada primjenom Kineske teoreme o ostatcima kako je pokazano u prethodnim zadacima dobijamo respektivno rješenja sistema:*
$\boxed{x = 112}$
$\boxed{x = 166}$
$\boxed{x = 251}$
$\boxed{x = 305}$
*Uvrštavajući ova rješenja u početnu kongruenciju dobijamo da je ona zadovoljena*

*d) Tražimo x koji je rješenje kongruencije* $x^2 \equiv 1836 \pmod{4185}$*, a za koji vrijedi* $0 \leq x < 4185$. ***NZD** (1836, 4185) = 27 ≠ 1*
*Potrebno je modul učiniti relativno prostim sa brojem sa desne strane kongruencije.*
*27 pišemo kao* $27 = 3 \cdot 3^2$ *odakle vidimo da je* $\boldsymbol{p = q = 3}$

*Smjenom* $x = pqy$ *dobijamo kongruenciju* $3y^2 \equiv 68 \pmod{155}$
*Sada zamijenimo* $y^2 = z$ *te riješimo pomoćnu kongruenciju* $3z \equiv \frac{1836}{27} \pmod{\frac{4185}{27}}$
*odnosno* $3z \equiv 68 \pmod{155}$
*pri rješavanju ove kongruencije dobijamo Diofantovu jednačinu* $3z + 155k = 68$
***NZD**(3, 155) = 1 a 1|68 pa je ona rješiva. Imamo:*
$1 = 52 \cdot 3 - 1 \cdot 155$
*pa odavde slijedi:*

$z \equiv 3536 \pmod{155}$ *odnosno nakon redukcije po modulu 155*
$z \equiv 126 \pmod{155}$

*Kako je* $y^2 = z$ *dobijamo kongruenciju*
$y^2 \equiv 126 \pmod{155}$
*Primjetimo da je* ***NZD**(126, 155) = 1 te 155 =* $5 \cdot 31$ *time dobijamo dvije pomoćne*

*kongruencije:*

$y^2 \equiv 126 \ (mod\ 5)$ *i* $y^2 \equiv 126 \ (mod\ 31)$

*Redukcijom prve kongruencije po modulu 5 dobijamo kongruenciju* $y^2 \equiv 1 \ (mod\ 5)$ *odakle su više nego očita rješenja* $\boldsymbol{y = 1}$ *i* $\boldsymbol{y = 4}$

*Također redukcijom druge kongruencije po modulu 31 dobijamo kongruenciju*

$y^2 \equiv 2 \ (mod\ 31)$

*kako je* $\boldsymbol{NZD}(2, 31) = 1$ *te ako primjetimo da je* $mod(31, 4) = 3$ *tako možemo primjeniti već navedenu Lagrangeovu formulu iz koje dobijamo rješenja*

$\boldsymbol{y = 8}$ *i* $\boldsymbol{y = 23}$

*Možemo izvući četiri sistema kongruencija:*

$y \equiv 1 \ (mod\ 5)$ *i* $y \equiv 8 \ (mod\ 31)$

$y \equiv 1 \ (mod\ 5)$ *i* $y \equiv 23 \ (mod\ 31)$

$y \equiv 4 \ (mod\ 5)$ *i* $y \equiv 8 \ (mod\ 31)$

$y \equiv 4 \ (mod\ 5)$ *i* $y \equiv 23 \ (mod\ 31)$

*Primjenom Kineske teoreme o ostatcima za date sisteme dobijamo redom rješenja:*

$\boxed{y = 101}$ $\boxed{y = 116}$ $\boxed{y = 39}$ $\boxed{y = 54}$

*Svakom ovom rješenju odgovara* $\boldsymbol{q}$ *tipičnih rješenja polazne kongruencije koja dobijamo po formuli* $pqy + (\frac{m}{q}) \cdot i$ *za* $i = 0, 1, \ldots, q - 1$

*gdje je nama* $\boldsymbol{q = 3}$ *pa redom dobijamo rješenja:*

$\boxed{x_1 = 909}$

$\boxed{x_2 = 2304}$

$\boxed{x_3 = 3699}$

$\boxed{x_4 = 1044}$

$\boxed{x_5 = 2349}$

$\boxed{x_6 = 3834}$

$\boxed{x_7 = 351}$

$\boxed{x_8 = 1746}$

$\boxed{x_9 = 3141}$

$\boxed{x_{10} = 486}$

$\boxed{x_{11} = 1881}$

$\boxed{x_{12} = 3276}$

*Uvrštavajući ova rješenja u početnu kongruenciju dobijamo da je ona zadovoljena.*

7. Alma i Bruno 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 = 673 i generator g = 17. Nakon toga, Alma je u tajnosti slučajno izabrala broj a = 296, dok se Bruno u tajnosti odlučio za broj

b = 241. Odredite koje još informacije Alma i Bruno moraju razmijeniti preko ETF Haber kutije da bi se dogovorili o vrijednosti ključa, te kako glasi ključ koji su oni dogovorili

*Znamo da su Alma i Bruno dogovorili oko izbora prostog broja i generatora, te dva slučajna broja u opsegu (0, p-1).*
*Da bi se dogovorili oko vrijednosti ključa, Alma mora Bruni poslati vrijednost* $\alpha = mod(g^a, p)$*, a Bruno njoj vrijednost* $\beta = (g^b, p)$.
*Zatim oboje mogu naći vrijednost ključa k, po sljedećim formulama:*
$k = mod(a^\beta, p)$ *- Alma, odnosno* $k = mod(b^\alpha, p)$ *- Bruno. Nađimo vrijednost* $\beta$*:*

$$\beta = mod(17^{241}, 673)$$

*primjenom kvadriraj i množi:*

$$\beta = (17^{128} \ mod \ 673 \cdot 17^{64} \ mod \ 673 \cdot 17^{32} \ mod \ 673 \cdot 17^{16} \ mod \ 673 \cdot 17^{1} \ mod \ 673) \ mod \ 673$$

*Imamo da je:*

$$([17]_{673})^2 = [289]_{673}$$
$$([289]_{673})^2 = [83521]_{673} = [69]_{673}$$
$$([69]_{673})^2 = [4761]_{673} = [50]_{673}$$
$$([50]_{673})^2 = [2500]_{673} = [481]_{673}$$
$$([481]_{673})^2 = [231361]_{673} = [522]_{673}$$
$$([522]_{673})^2 = [272484]_{673} = [592]_{673}$$
$$([592]_{673})^2 = [350464]_{673} = [504]_{673}$$

*Odnosno* $\beta = [17 \cdot 481 \cdot 522 \cdot 592 \cdot 504]_{673}$

$$\boxed{\beta = 391}$$

*Ponovimo li isti postupak i za* $\alpha$*, dobit ćemo:*

$$\boxed{\alpha = 380}$$

*Preostaje nam da izračunamo ključ k preko obje formule i uporedimo rješenja:*
*1.* $k_1 = mod(\beta^a, p)$

$k_1 = mod(391^{296}, 673)$ *koji se također računa primjenom kvadriraj i množi gdje dobijamo da nam je:*

$$\boxed{k_1 = 466}$$

*Analogno* $k_2 = mod(\alpha^b, p)$

$k_1 = mod(380^{241}, 673)$ *odnosno* $\boxed{k_2 = 466}$

*Očigledno da je ključ u ovoj razmjeni poruka* $k = 466$*, vrijedi* $k_1 = k_2$*, pa je on valjan.*
*Dakle,*
*Alma i Bruno su dogovorili ključ* $k = 466$*, nakon što su razmijenili vrijednosti* $\alpha$ *i* $\beta$*.*

8. Adrijana i Bilal međusobno razmjenjuju poruke preko Facebook-a. Kako je poznato da takva komunikacija nije pouzdana, oni su odlučili da će primati samo šifrirane poruke. Adrijana je na svoj profil postavila informaciju da prima samo poruke šifrirane pomoću RSA kriptosistema s javnim ključem (869, 1763), dok je Bilal postavio informaciju da prima samo poruke šifrirane RSA kriptosistemom s javnim ključem (529, 629).

- Odredite kako glase tajni ključevi koje koriste Adrijana i Bilal za dešifriranje šifriranih poruka koje im pristižu.
- Odredite kako glase funkcije šifriranja i dešifriranja koje koriste Adrijana i Bilal za šifriranje poruka koje šalju jedno drugom, odnosno za dešifriranje šifriranih poruka koje im pristižu.
- Odredite kako glasi šifrirana poruka y koju Adrijana šalje Bilalu ako izvorna poruka glasi x = 2912. Kako glasi digitalni potpis z u slučaju da Adrijana želi Bilalu dokazati da poruka potiče baš od nje?
- Pokažite kako će Bilal dešifrirati šifriranu poruku y koju mu je Adrijana poslala (tj. primijenite odgovarajuću funkciju za dešifriranje na šifriranu poruku) i na osnovu primljenog digitalnog potpisa z utvrditi da je poruka zaista stigla od Adrijane.

*Imamo da je Adrijanin javni ključ (869, 1763) a Bilalov (529, 629)*
*Prema RSA protokolu, funkcija za šifriranje poruka prema/za Adrijanu je:*

$$E_{A(x)} = mod(x^{869}, 1763)$$

*Dok je funkcija za šifriranje poruka prema/za Bilala:*

$$E_{B(x)} = mod(x^{529}, 629)$$

*Za nalaženje funkcija dešifriranja $D_{A(y)}$ i $D_{B(y)}$ trebamo naći tajne eksponente odnosno $b_A$ i $b_B$*
*Za ovo nam trebaju vrijednosti $\varphi(1763)$ kao i $\varphi(629)$*
*Kako rastava broja 1763 na proste faktore glasi*
$1763 = 41 \cdot 43$ *odavde nam je lahko izračunati* $\varphi(1763) = (41-1)\cdot(43-1) = 1680$
*analogno imamo da je* $\varphi(629) = 576$

*Sada se $b_A$ i $b_B$ dobiju kao tipična rješenja kongruencija :*

$$869b_A \equiv 1 \ (mod\ 1680) \ \textit{odnosno}\ 529b_B \equiv 1 \ (mod\ 576)$$

*Rješavanjem njima pripadajućih Diofantovih jednačina koje su mnogo puta do sada u ovom dokumentu rješavane dobijamo redom rješenja:*

$$\boxed{b_A = 29} \ i \ \boxed{b_B = 49}$$

*Sada funkcije dešifriranja glase:*

$$D_{A(y)} = mod(y^{29}, 1763) \ i \ D_{B(y)} = mod(y^{49}, 629)$$

*odavde slijedi da je Adrijanin tajni ključ (29, 1763) a Bilalov (49, 629)*

*Sada Adrijana Bilalu šalje poruku $\boldsymbol{x = 2912}$, pa je šifriramo odnosno računamo*

$$E_{B(2912)} = mod(2912^{529}, 629)$$

*kako je* $2912 > 629$ *moramo broj 2912 napisati u bazi 629 što nije teško jer imamo da je:*
$2912 = 4 \cdot 629 + 396$ *odakle moramo izračunati* $E_{B(4)} = mod(4^{529}, 629) = 548$
*i* $E_{B(396)} = mod(396^{529}, 629) = 396$ *sada y rekonstruišemo kao:*

$$y = 548 \cdot 629 + 396$$

*odnosno dobijamo da šifrirana poruka koju Adrijana šalje Bilalu glasi:*

$\boxed{y = 345088}$

*Sada izračunajmo Adrijanin digitalni potpis.*
*Njega računamo kao:*

$$z = E_B(D_A(2912))$$

*označimo* $D_A$ *sa u.*
*Imamo* $u = mod(2912^{29}, 1763)$*, te opet kako je 2912 > 1763 napišimo 2912 u bazi 1763.*
*Imamo:*

$$2912 = 1 \cdot 1763 + 1149$$

*Analogno prethodno pokazanom koraku računajući* $D_A(1)$ *i* $D_A(1149)$ *dobijamo da je:*

$u = 1 \cdot 1763 + 616$ *odnosno* $\boxed{u = 2379}$

*Sada imamo da je* $z = E_B(2379)$ *gdje opet uvidjevši funkciju* $E_B$ *primjećujemo da ćemo opet morati ponavljati haman te isti postupak ko maloprije i da ćemo rekonstruisati na isti način z, pa ćemo samo napisati rezultat za Adrijanin digitalni potpis jer sam fakat slomljen od silnih zadaća :( (RI2 is more like RIP2)*

*Helem, Adrijanin digitalni potpis iznosi:*

$\boxed{z = 259011}$

*Bilal sada mora dešifrirati poruku* $y = 345088$ *koju je primio primjenom svoje funkcije dešifrovanja i dobija:*
$x = mod(345088^{49}, 629)$ *te ponovo ista priča kako je 345088 > 629, moramo 345088 predstaviti u bazi 629 pa imamo;*

$$345088 = 548 \cdot 629 + 396$$

*Računajući* $D_B(548)$ *i* $D_B(396)$ *dobijamo da dešifrovana poruka* $y = 345088$ *glasi:*
$x = 4 \cdot 629 + 396$ *odnosno* $\boxed{x = 2912}$ *što je jednako originalnoj poruci koju je Adrijana poslala Bilalu.*

*Sada još moramo utvrditi da li je zaista ta poruka koju je Bilal dobio, došla od Adrijane.*
*Kako bi to provjerili računamo :*

$E_A(D_B(z))$ *odnosno* $E_A(D_B(259011))$

*gdje očigledno moramo prvo izračunati* $D_B(259011) = mod(259011^{49}, 629) = q = 2379$
*(postupak isti kao i prethodni gdje se mora rekonstruisati q jer je 259011 > 629)*

*Sada računamo* $E_A(2379) = mod(2379^{869}, 1763)$ *gdje je ista priča sa rekonstrukcijom ko i ranije (jer je 2379 > 1763).*
*Nakon obavljene rekonstrukcije dobijamo da je:*

$$x = 1 \cdot 1763 + 1149$$

*odnosno*

$\boxed{x = 2912}$

*pa sa sigurnošću znamo da je Bilal poruku primio od Adrijane!*