Fakulteta za matematiko in fiziko

Elementarna teorija števil

Nace Zavrtanik

2016/2017

Nastanek teh skript je motivirala predvsem želja po urejenih zapiskih pri predmetu Elementarna teorija števil, delno pa sem želel tudi olajšati študij tega predmeta svojim kolegom. Snov je v celoti povzeta po predavanjih profesorja Saša Strleta, kot jo je predaval v študijskem letu 2016/17. Moja skromna vloga pri nastanku tega teksta je večinoma ta prepisovalca, ponekod pa tudi dopolnim dokaze, ki so na predavanjih bili izpuščeni bodisi zaradi preproste narave bodisi zaradi obravnave pri predmetih, ki naj bi na tej točki že bili opravljeni.

Kazalo

1 Uvod **3**
- 1.1 Številske množice . . . 3
- 1.2 Deljivost . . . 4
- 1.3 Diofantske enačbe in verižni ulomki . . . 6

2 Naravna števila **7**
- 2.1 Peanovi aksiomi . . . 7
- 2.2 Vpeljava operacij . . . 7
- 2.3 Urejenost . . . 8
- 2.4 Vložitev naravnih števil v cela števila . . . 10
- 2.5 Vložitev celih števil v racionalna števila . . . 11
- 2.6 Vložitev racionalnih števil v realna števila . . . 11

3 Deljivost **11**
- 3.1 Osnovni izrek o deljenju . . . 11
- 3.2 Vsote kvadratov celih števil . . . 12
- 3.3 Lastnosti in največji skupni delitelj . . . 14

4 Diofantske enačbe **16**

5 Multiplikativne funkcije **16**

6 Kongruence **16**
- 6.1 Definicija in osnovne lastnosti . . . 16
- 6.2 Kriteriji za deljivost . . . 18
- 6.3 Reducirani sistem ostankov . . . 20
- 6.4 Rešljivost linearih kongruenc . . . 20
- 6.5 Sistemi linearnih kongruenc . . . 22
- 6.6 Eulerjeva funkcija ϕ . . . 25
- 6.7 Polinomske kongruence . . . 28

7 Kriptografija **29**
- 7.1 Afina šifra . . . 29
- 7.2 Hillova šifra . . . 31
- 7.3 Ideja o javnih ključih . . . 31
- 7.4 Algoritem RSA . . . 32

1 Uvod

Samo ime predmeta, Elementarna teorija števil, nakazuje na to, da bomo števila preučevali z elementarnimi sredstvi, t. j. z znanjem, ki je bilo osvojeno že pri Analizi 1, Algebri 1 in Algebri 2. Toda kaj matematiki sploh razumemo kot števila?

1.1 Številske množice

Definicija 1. ***Številska množica*** *je množica, opremljena z operacijama seštevanja "* $+$ *" in množenja "* $\cdot$ *".*

Primer: $\mathbb{N}$, $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{H}$.

Operaciji $+$ in $\cdot$ imata neke lastnosti, same številske množice pa razlikujemo na podlagi tega, kako daleč sta operaciji od tega, da bi bili "lepi". Tako so naravna števila zgolj polgrupa, s priključitvijo elementa 0 postanejo monoid, cela števila so kolobar, racionalna in realna števila pa polje. Z dodajanjem ustreznih elementov tako prehajamo s preprostih na naravno sledeče algebrske strukture. Tukaj velja omeniti, da pa prehod z racionalnih na realna števila ni algebrske narave, temveč topološke, saj je $\mathbb{R}$ ravno napolnitev topološkega prostora $\mathbb{Q}$.

V teoriji števil nas številske množice od $\mathbb{Q}$ naprej ne bodo zanimale, saj se bomo ukvarjali predvsem z *aritmetičnimi* lastnostmi števil, t. j. z lastnostmi, povezanimi z deljivostjo. Ukvarjali se bomo z elementi, ki nimajo multiplikativnega inverza, zato obsegov, v katerih je obrnljiv vsak element, ne bomo obravnavali. To nas pripelje do naslednje definicije:

Definicija 2. *Naj bo* K *kolobar in* $a \in K$*. Element* a *je* ***enota****, če ima multiplikativni inverz.*

Od tod pride pojem praštevila, ki je osnova pri študiju naravnih števil. Poleg $\mathbb{N}$ in $\mathbb{Z}$ pa obstajajo še številne druge številske množice, ki so podmnožice katerega od zgorjih obsegov.

Primer:

1. $\mathbb{Z}[\frac{1}{2}] = \{a_0 + a_1\frac{1}{2} + a_2(\frac{1}{2})^2 + \cdots + a_n(\frac{1}{2})^n \mid \forall i.a_i \in \mathbb{Z}, n \in \mathbb{N}_0\}$

   Velja $\mathbb{Z} \leq \mathbb{Z}[\frac{1}{2}] \leq \mathbb{Q}$.

   V kolobar $\mathbb{Z}$ smo dodali inverz števila 2. S tem je število 2 postalo enota.

2. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

   Velja $\mathbb{Z} \leq \mathbb{Z}[\sqrt{2}] \leq \mathbb{R}$.

3. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

   Velja $\mathbb{Z} \leq \mathbb{Z}[i] \leq \mathbb{C}$.

   Množico $\mathbb{Z}[i]$ imenujemo tudi *Gaußova cela števila*.

Sedaj, ko imamo številske množice, lahko na njih definiramo relacijo deljivosti.

1.2 Deljivost

Definicija 3. *Naj bo S številska množica in $a, b \in S$. Pravimo, da b **deli** a, če obstaja taki $c \in S$, da velja $a = b \cdot c$. Pišemo $b|a$.*

Primer: Za različne številske množice S bomo poiskali delitelje števila $a = 2$:

1. $S = \mathbb{N}$:

   $b|a$, če velja $b = 1$ ali $b = 2$.

2. $S = \mathbb{Z}$:

   $b|a$, če velja $b = \pm 1$ ali $b = \pm 2$.

   V $\mathbb{Z}$ imamo več deliteljev kot v $\mathbb{N}$, saj je v $\mathbb{Z}$ več enot. Poleg števila 1 je obrnljivo namreč tudi število -1.

3. $S = \mathbb{Z}[\frac{1}{2}]$:

   $b|a$, če velja $b = \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}, \ldots$ ali $b = \pm 1, \pm 2, \pm 4, \pm 8, \ldots$, torej

   $$b = \pm 2^n, n \in \mathbb{N}.$$

   Opazimo, da so v S vsa ta števila spet enote, saj za $c = \mp 2^{1-n}$ velja $b \cdot c = 2$.

4. $S = \mathbb{Z}[\sqrt{2}]$:

   $b|a$, če velja $b = \pm 1, \pm\sqrt{2}, \pm 2, \pm(2 \pm \sqrt{2})$.

   Hitro preverimo, da zgornja števila res delijo a. Pojavi pa se vprašanje, ali so to res *vsi* delitelji za a. V prejšnjih primerih smo tudi opazili, da če b deli a, potem za poljubno enoto e produkt $b \cdot e$ prav tako deli a. Zato se dodatno vprašamo, ali so zgornji delitelji za a bistveno različni v smislu, da se ne razlikujejo le za enoto.

Odgovorimo najprej na drugo vprašanje:

$$2 + \sqrt{2} = \sqrt{2}(\sqrt{2} + 1)$$

Ker velja $(\sqrt{2}+1)\cdot(\sqrt{2}-1) = 1$, se delitelja $\sqrt{2}$ in $\sqrt{2}+1$ res razlikujeta le za enoto.

Če želimo poiskati še vse delitelje, moramo poiskati vse enote. Iščemo torej take $a, b \in \mathbb{Z}$, da bo $a + b\sqrt{2}$ enota (tukaj sta a in b neznanki in nista povezani s številom a in njegovimi delitelji b iz primera).

$$\exists c, d \in \mathbb{Z}.(a + b\sqrt{2})(c + d\sqrt{2}) = 1$$

Ta enačba je ekvivalenta enačbi

$$ac + 2bd - 1 = -\sqrt{2}(ad + bc),$$

za katero vemo, da je njena leva stran cela, saj so cela števila zaprta za seštevanje in množenje. Za desno stran pa lahko trdimo, da bo iracionalna, razen pod pogojem, da je $ad + bc = 0$. Veljati mora torej $ad = -bc$, kar je gotovo res, če $c = a$ in $d = -b$, če $c = k \cdot a$ in $d = -b \cdot k$ ali simetrično $a = l \cdot c$ in $b = -l \cdot d$. Pokazali bomo, da lahko velja le prva izmed teh treh možnosti. Če v zgornjo enačbo vstavimo pogoj $ad + bc = 0$, dobimo enakost $ac + 2bd = 1$. S pomočjo te enakosti lahko razmislimo, da sta si števili a in b tuji:

Naj bo $a = a_1 e$ in $b = b_1 e$. Sledi $e(a_1 c + 2b_1 d) = 1$, zato po definiciji $e|1$. Število e je torej bodisi 1 bodisi -1, a in b pa sta si posledično tuji. Analogno lahko sklepamo, da sta si tuji tudi števili c in d.

Ker smo prepostavili $ad = -bc$, sledi, da $a|bc$, ker pa sta a in b tuji si števili, mora veljati $a|c$. Simetrično pokažemo, da $c|a$, od koder sklepamo, da res velja možnost $a = c$ in $b = -d$. Če sedaj dobljeni zvezi vstavimo v enakost $ac + 2bd = 1$, dobimo **Pellovo enačbo**

$$a^2 - 2b^2 = 1.$$

Vse enote v $\mathbb{Z}[\sqrt{2}]$ so celoštevilske rešitve te Pellove enačbe.

5. $S = \mathbb{Z}[i]$:

   $b|a$, če velja $b = \pm 1, \pm 2, \pm 1 \pm i, \ldots$

Ti primeri motivirajo definicijo:

Definicija 4. *Naj bo S številska množica in $a \in S$. Element a je* ***nerazcepen****, če iz $a = bc$ sledi, da je vsaj eden od elementov b in c enota.*

Opomba: V $S = \mathbb{N}$ so nerazcepni elementi, ki niso enote, praštevila.

Definicija 5. *Naj bo S številska množica in $a \in S$. Element a je* ***primitivni element*** *ali* ***praelement****, če iz $a|bc$ sledi $a|b$ ali $a|c$.*

Opomba: V $S = \mathbb{N}$ tudi to določa praštevila.

Opomba: V splošnem pojma nerazcepnega in primitivnega elementa nista ekvivalentna:
$S = \mathbb{Z}[\sqrt{2}, i]$:
$2 = \sqrt{2} \cdot \sqrt{2} = (1+i)(1-i)$, torej $\sqrt{2}|(1+i)(1-i)$, vendar $\sqrt{2} \nmid (1+i)$ in $\sqrt{2} \nmid (1-i)$.

1.3 Diofantske enačbe in verižni ulomki

Pri teoriji števil nas bodo zanimale tud celoštevilske rešitve diofantskih enačb.

Definicija 6. ***Diofantska enačba*** *je polinomska enačba s celimi koeficienti.*

Primer:

1. linearne diofantske enačbe: $ax + by = c$, kjer $a, b, c \in \mathbb{Z}$
2. pitagorejske trojice: $x^2 + y^2 = z^2$
3. Pellova enačba: $y^2 - ax^2 = 1$
4. $x^2 + y^2 = a$

Enačbi v 3. in 4. primeru sta primera binarnih kvadratnih form nad $\mathbb{Z}$.

Spomnimo se: Če je M kvadratna forma nad $\mathbb{R}$, ima same realne lastne vrednosti (v splošnem so kompleksne), pripadajoči lastni vektorji pa so linearno neodvisni. Posledično obstaja baza iz lastnih vektorjev, kar pomeni, da lahko M diagonaliziramo. Za kvadratne forma nad $\mathbb{Z}$ to ne velja in so v splošnem veliko bolj zakomplicirane.

Še en objekt, ki ga bomo študirali pri teoriji števil, so **verižni ulomki**, o katerih bomo več povedali kasneje.

2 Naravna števila

Naravna števila $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ so prva številska množica, s katero se srečamo pri učenju matematike, in ponavadi jih opišemo kar kot "števila, s katerimi štejemo". Nas bo zanimala formalna definicija naravnih števil, ki bo opisala bistvene lastnosti te številske množice.

2.1 Peanovi aksiomi

Definicija 7 (Peanovi aksiomi)**.** ***Množica naravnih števil*** *je množica N skupaj s funkcijo $\phi : N \to N$, ki vsakemu elementu $n \in \mathbb{N}$ priredi svojega* ***neposrednega naslednika****. Množica N mora ustrezati naslednjim aksiomom:*

P1. $\exists \epsilon \in N. \epsilon \neq \phi(n)$

P2. Funkcija ϕ je injektivna.

P3. Za podmnožico $A \subseteq N$ velja: če $\epsilon \in A$ in če je za vsak $n \in A$ tudi $\phi(n) \in A$, potem velja $A = N$.

Opomba: Aksiom *P3* je načelo popolne matematične indukcije.

Kako pa množica N iz definicije sploh izgleda? Iz *P1* sledi

$$N \supseteq \{\epsilon, \phi(\epsilon), \phi(\phi(\epsilon)), \dots\}.$$

V množici N imamo torej ϵ in vse njegove naslednike, vendar bi N lahko vsebovala še katera druga števila. Šele aksiom *P3* nam zagotovi, da je v zgornjem izrazu v bistvu kar enakost. Velja torej

$$N = \{\epsilon, \phi(\epsilon), \phi(\phi(\epsilon)), \dots\}.$$

Sedaj lahko za elemente množice N vpeljemo oznake, ki so nam bliže za operiranje s števili, in sicer $1 := \epsilon, 2 := \phi(\epsilon), 3 := \phi(\phi(\epsilon))$, itn. Včasih nam ustreza tudi število nič obravnavati kot naravno število. V tem primeru podobno definiramo $0 := \epsilon, 1 := \phi(\epsilon), 2 := \phi(\phi(\epsilon))$, itn.

2.2 Vpeljava operacij

Sedaj vemo, kaj so elementi naše množice naravnih števil N, da bo zares postala številska množica, pa je potrebno definirati še operaciji seštevanja "$+$" in množenja "$\cdot$". Operaciji definiramo induktivno na sledeč način:

$$n + \epsilon := \phi(n)$$
$$n + m := \phi(n + m)$$

$$n \cdot \epsilon := n$$
$$n \cdot \phi(n + m) := n \cdot m + n$$

Iz teh definicij lahko določimo osnovne lastnosti računskih operacij. Te so asociativnost, komutativnost, distributivnost in pa pravili krajšanja. Pravili krajšanja se glasita:

$$n + l = m + l \Rightarrow n = m$$
$$n \cdot l = m \cdot l \Rightarrow n = m$$

Pokazali bomo, do prvo pravilo krajšanja res velja, drugo pa se dokaže na podoben način. Dokaza se bomo lotili z indukcijo po l. V nadaljevanju bomo uporabljali standardne oznake za naravna števila, samo množico bomo pa označevali z $\mathbb{N}$.

$$l = 1 : \; n + 1 = m + 1 \iff \phi(n) = \phi(m) \overset{inj.}{\Longrightarrow} n = m \; \checkmark$$

$$l \to l + 1 : \; n + \phi(l) = m + \phi(l) \iff \phi(n + l) = \phi(m + l) \overset{inj.}{\Longrightarrow} n + l = n + m \overset{I.P.}{\Longrightarrow} n = m \; \checkmark$$

2.3 Urejenost

S pomočjo operacij v množico naravnih števil $\mathbb{N}$ uvedemo urejenost. Za elementa $n, m \in \mathbb{N}$ definiramo relaciji $<$ in $\leq$ na sledeč način:

$$n < m \iff \exists k \in \mathbb{N}. n + k = m$$
$$n \leq m \iff n < m \text{ ali } n = m$$

Relacijo $>$ (in $\geq$) smiselno definiramo kot negacijo $\leq$ (in $<$).

Trditev 1. *Za vsak $n \in \mathbb{N}$ velja $1 \leq n$ in množica $\mathbb{N}$ je linearno urejena.*

Spomnimo se: Relacija R je relacija linearne urejenosti na množici A, če za vsake $a, b, c \in A$ velja:

1. *refleksivnost:* $a\ R\ a$
2. *antisimetričnost:* $a\ R\ b$ in $b\ R\ a \implies a = b$
3. *tranzitivnost:* $a\ R\ b$ in $b\ R\ c \implies a\ R\ c$
4. *sovisnost:* $a\ R\ b$ ali $b\ R\ a$

Pri dokazu linearne urejenosti bomo dokazali le varianto sovisnosti, ki pravi, da za $n, m \in \mathbb{N}$ velja natanko ena izmed možnosti $n = m$, $n < m$ ali $m < n$.

Dokaz. Prvi del izreka bomo dokazali z indukcijo.

$n = 1$: $1 \leq 1$ ✓

$n \to n + 1$: Poljubno naravno število $n \neq 1$ je oblike $n = \phi(m) = m + 1$ za neki naravni m. Velja $1 < 1 + m = n$. ✓

Za dokaz linearne urejenosti bomo ločili tri primere, in sicer:

$n = m$: Če bi veljalo $n < m$, bi po definiciji relacije $<$ obstajal neki $k \in \mathbb{N}$, da bi veljalo $n + k = m = n$. Če sedaj $n = 1$, dobimo $1 = 1 + k = \phi(k)$, kar je protislovje s Peanovim aksiomom *P1.* Če je pa $n > 1$, velja $n = \phi(l) = l + 1$ za neki naravni l. Sledi $l + 1 + k = l + 1 \xRightarrow[krajšanja]{pravilo}$ $1 + k = \phi(k) = 1$, kar pa je spet protislovje s *P1.* Pridemo do sklepa, da ne velja $n < m$, simetrično pa sklepamo tudi $m < n$. Velja torej res natanko ena izmed možnosti $n = m$, $n < m$ ali $m < n$.

$n \neq m$ in $n < m$: Če bi veljalo $m < n$, bi spet obstajal neki $l \in \mathbb{N}$, da bi veljalo $n = m + l$. Po predpostavki $n < m$ obstaja $k \in \mathbb{N}$, da velja $n + k = m$. Iz obeh enakosti sledi

$$(m + l) + k = m \text{ in}$$
$$m + (l + k) = m,$$

kar nas pripelje do istega protislovja kot v zgornjem primeru.

$n \neq m$ in $\neg(n < m)$: Pokazati moramo, da velja možnost $m < n$. Definirajmo množici

$$A_1 := \{1, 2, \ldots, m - 1\} \text{ in}$$
$$A_2 := \{m + 1, m + 2, \ldots\}.$$

Ker so vsa števila v množici A_1 manjša od m, gotovo $n \notin A_1$. Po predpostavki prav tako velja $n \neq m$. Množica $A := A_1 \cup \{m\} \cup A_2$ zadošča pogojem v Peanovem aksiomu *P3*, kar implicira $A = \mathbb{N}$. Ker $n \in A$ in $n \notin A_1, n \neq m$, sledi $n \in A_2$ oz. $m < n$.

□

Definicija 8. *Množica A je **dobro urejena**, če ima vsaka neprazna podmnožica $S \subseteq A, S \neq \emptyset$, najmanjši element.*

Izrek 1. *Množica naravnih števil $\mathbb{N}$ je dobro urejena.*

Dokaz. Naj bo $S \subseteq \mathbb{N}, S \neq \emptyset$. Ločili bomo primera, ko $1 \in S$ in ko $1 \notin S$:

$1 \in S$: Trditev 1 nam pove, da $1 \leq n$ za vsak $n \in \mathbb{N}$, torej je kar število 1 iskani najmanjši element množice S.

$1 \notin S$: Tukaj bomo obstoj najmanjšega elementa pokazali s protislovjem. Predpostavimo torej, da množica S nima najmanjšega elementa. Ker $S \neq \emptyset$, obstaja $n_0 \in S$, ki pa ni najmanjši element množice S. Obstaja torej $n_1 \in S, n_1 < n_0$. Ker S nima najmanjšega elementa, podobno obstaja $n_2 \in S, n_2 < n_1$. Postopek ponavljamo in pridemo do rezultata, da množica S vsebuje neskončno elementov, ki so manjši od n_0. To nas pripelje v protislovje, saj lahko množica S vsebuje kvečjemu $n_0 - 2$ elementov, ki so manjši od n_0 (1 namreč ni element S).

□

Opomba: Dobra urejenost je ekvivalentna Peanovemu aksiomu *P3*.

2.4 Vložitev naravnih števil v cela števila

Naravno števila lahko vložimo v cela števila.

$$\mathbb{N} \hookrightarrow \mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n \mid n \in \mathbb{N}\}$$

Seštevanje definiramo na sledeč način:

$$n + (-m) := \begin{cases} k & ; n > m, \text{ kjer } n = m + k \\ -k & ; n < m, \text{ kjer } m = n + k \end{cases}$$

Vse lastnostni operacij se ohranijo, pridobimo pa inverze za seštevanje.

Urejenost lahko prenesemo z naravnih števil tako, da za vsaka $x, y \in \mathbb{Z}$ identično definiramo

$$x < y \iff \exists k \in \mathbb{N}.\ x + k = y.$$

Opomba: Naj bo $n < m,\ n, m \in \mathbb{N}$. Po definiciji obstaja $k \in \mathbb{N}$, da velja $n + k = m$. Od tod sledi $(-m) + k = (-n)$, kar pomeni, da $-m < -n$. Opazimo torej, da se neenačaj pri "množenju z -1"obrne.

2.5 Vložitev celih števil v racionalna števila

Cela števila lahko vložimo v racionalna števila.

$$\mathbb{Z} \hookrightarrow \mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}/\sim$$

Množica $\mathbb{Q}$ je torej kvocientna množica, kjer je ekvivalenčna relacija $\sim$ definirana takole:

$$\frac{m_1}{n_1} \sim \frac{m_2}{n_2} \iff m_1 n_2 = n_1 m_2.$$

2.6 Vložitev racionalnih števil v realna števila

Racionalna števila lahko vložimo v realna števila.

$$\mathbb{Q} \hookrightarrow \mathbb{R}$$

Množica $\mathbb{R}$ je napolnitev topološkega prostora $\mathbb{Q}$ v standardni metriki.

3 Deljivost

Spomnimo se, da b deli a, $b|a$, če obstaja tak $c \in \mathbb{Z}$, da velja $a = b \cdot c$. Iz pravila krajšanja sledi, da je ta c za $b \neq 0$ enolično določen. Kaj pa, če $b \nmid a$? Več o tem nam pove naslednji izrek.

3.1 Osnovni izrek o deljenju

Izrek 2 (Osnovni izrek o deljenju)**.** *Naj bo $a \in \mathbb{Z}$ in $b \in \mathbb{N}$. Potem obstajata enolično določeni števili $q, r \in \mathbb{Z},\ 0 \leq r < b$, da velja*

$$a = q \cdot b + r.$$

Dokaz. Definirajmo množico $R := \{a - nb \mid n \in \mathbb{Z},\ a - nb \geq 0\}$. Razmislimo, da tako definirana množica R ni prazna. Če je $a > 0$, lahko izberemo $n = 0$ in je tako $a \in R$. Če pa je $a < 0$, lahko vzamemo $n = a$ in tako dobimo $a - ab = a(1 - b) \geq 0$, saj je $1 - b \leq 0$.
Sedaj bomo ločili primera, ko $0 \in R$ in $0 \notin R$:

- $0 \in R$:

  Iz definicije množice R sledi $a - nb = 0$, oz. $a = nb$. To je že zapis želene oblike, in sicer za $r = 0$.

- $0 \notin R$:

  Ker $0 \notin R$, je $R \subset \mathbb{N}$. Pokazali smo že, da je množica R neprazna, torej lahko uporabimo načelo dobre urejenosti, ki nam pove, da ima množica R najmanjši element. Označimo ta najmanjši element z r. Velja $r = a - nb$, kar je enako $a = nb + r$. Pokažimo še, da $r < b$.

  Če $r \geq b$, bi obstajal $r_1 \geq 0$, da bi veljalo $r = r_1 + b$. Naprej bi lahko sklepali $a - nb = r = r_1 + b$, kar je ekvivalentno enakosti $a - (n+1)b = r_1$. Slednje bi pomenilo, da je $r_1 \in R$, kar pa bi bilo v protislovju s tem, da je r najmanjši element množice R.

  Preostane še pokazati, da sta števili q in r enolično določeni. Naj velja $a = qb + r = q_1 b + r_1$, kjer $q, q_1, r, r_1 \in \mathbb{Z}$ in $0 \leq r, r_1 < b$. Sledi

$$\begin{aligned} qb - q_1 b &= r_1 - r \\ (q - q_1)b &= r_1 - r \implies b|(r_1 - r) \end{aligned}$$

  Iz predpostavke $0 \leq r, r_1 < b$ sledi $-b < r_1 - r < b$, torej mora veljati $r_1 - r = 0$, od koder takoj sledi tudi $q - q_1 = 0$.

□

Posledica: Za $m \in \mathbb{Z}$ lahko vsako celo število zapišemo na enega izmed sledečih načinov:

$$km,\ km + 1,\ km + 2, \ldots,\ km + (m - 1)$$

za neki $k \in \mathbb{Z}$. Množice $[r] = \{km + r \mid k \in \mathbb{Z}\}$ imenujemo **kongruenčni razredi** po modulu m za $r = 0, 1, 2, \ldots, m - 1$. Števila $0, 1, 2, \ldots, m - 1$ imenujemo **standardni popolni sistem ostankov** po modulu m. Če izberemo po en element iz posameznega kongruenčnega razreda, tako dobimo poljubni popolni sistem ostankov po modulu m. Če a in b pripadata istemu kongruenčnemu razredu po modulu m, pišemo

$$a \equiv b \pmod{m}.$$

Popolnim sistemom ostankov in kongruencam se bomo podrobneje posvetili v poglavju 6.

3.2 Vsote kvadratov celih števil

Na tem mestu si bomo ogledali nekaj lastnosti vsot kvadratov celih števil, kasneje pa bomo to področje raziskali veliko bolj temeljto.

Trditev 2. *Če lahko $n \in \mathbb{N}$ zapišemo kot vsoto dveh kvadratov celih števil, t.j. če ima enačba $x^2 + y^2 = n$ celoštevilski rešitvi x in y, potem $n \not\equiv 3 \pmod 4$.*

Dokaz. Ogledali si bomo, kakšni so možni ostanki modulo 4 pri kvadriranju celega števila.

- $x = 2k : \; x^2 = 4k^2 \implies x^2 \equiv 0 \pmod 4$
- $x = 2k + 1 : \; x^2 = 4k^2 + 4k + 1 \implies x^2 \equiv 1 \pmod 4$

Možna ostanka pri deljenju kvadrata s 4 sta torej samo 0 in 1. Sledi

$$x^2 + y^2 \equiv \begin{cases} 0 \pmod 4 & ; \; x^2 \equiv y^2 \equiv 0 \pmod 4 \\ 2 \pmod 4 & ; \; x^2 \equiv y^2 \equiv 1 \pmod 4 \\ 1 \pmod 4 & ; \; \text{sicer} \end{cases}$$

□

Naravno se pojavi vprašanje, ali trditev drži tudi v drugo smer, t.j. ali lahko vsako število n, $n \not\equiv 3 \pmod 4$, zapišemo kot vsoto dveh kvadratov celih števil. Hitro najdemo primer, kjer to ne drži – število 6 namreč ni vsota kvadratov nobenih dveh celih števil. Vidimo pa, da nam vsota treh kvadratov lahko da vse možne ostanke modulo 4, kar nas napelje na razmislek o tem, katera števila lahko zapišemo kot vsoto treh kvadratov celih števil. V ta namen si bomo spet ogledali ostanke kvadratov, tokrat po modulu 8:

$$\begin{aligned} x \equiv 0 \pmod 4 &\implies x^2 \equiv 0 \pmod 8 \\ x \equiv 1 \pmod 4 &\implies x^2 \equiv 1 \pmod 8 \\ x \equiv 2 \pmod 4 &\implies x^2 \equiv 4 \pmod 8 \\ x \equiv 3 \pmod 4 &\implies x^2 \equiv 1 \pmod 8 \end{aligned}$$

Vidimo, da dobimo le ostanke 0, 1 in 4. Če sklepamo podobno kot v dokazu zgornje trditve, ugotovimo, da so možni ostanki vsote treh kvadratov po modulu 8 naslednji: 0, 1, 2, 3, 4, 5, 6. Sledi, da števila $n \equiv 7 \pmod 8$ ne moremo zapisati kot vsote treh kvadratov celih števil. Za razliko od prej pa tukaj velja obrat, ki ga bomo navedli brez dokaza:

Trditev 3. *Če je $n \not\equiv 7 \pmod 8$, lahko n zapišemo kot vsoto treh kvadratov celih števil.*

Brez dokaza bomo navedli tudi sledeči zrek:

Izrek 3. *Vsako naravno število je možno zapisati kot vsoto štirih kvadratov celih števil.*

3.3 Lastnosti in največji skupni delitelj

Trditev 4. *Vsako naravno število $n \in \mathbb{N}$ ima le končno mnogo deliteljev.*

Dokaz. Pokazali bomo nekaj več, in sicer to, da je vsak delitelj števila n manjši ali enak številu n,

$$d|n \implies d \leq n, \qquad (*)$$

od koder takoj sledi resničnost trditve. Če za d izberemo 1 ali n, implikacija $(*)$ očitno drži, zato bomo predpostavili $d \neq 0$ in $d \neq n$. Ker $d|n$, obstaja $k \in \mathbb{N}$, da $n = kd$. Če bi bil $k = 1$, bi bil $d = n$, torej mora vejati $k \geq 2$. Sledi $n = kd = d + (k-1)d$, kar po definiciji pomeni, da $d < n$, saj je $(k-1)d$ naravno število. □

Definicija 9. *Naj bosta $a, b \in \mathbb{Z}$ in ne obe enaki 0. Njun* ***največji skupni delitelj*** *d ali največjo skupno mero označimo*

$$d = nsd(a, b) = gcd(a, b) = (a, b).$$

(nsd... največji skupni delitelj, gcd... greatest common divisor)

Izrek 4. *Naj bosta $a, b \in \mathbb{Z}$ in ne obe enaki 0. Potem je njun največji skupni delitelj najmanjše naravno število v množici $D = \{ax + by \mid w, y \in \mathbb{Z}\}$.*

Dokaz. Najprej moramo pokazati, da v množici D najmanjše naravno število sploh obstaja. Želeli bi se ponovno sklicati na načelo dobre urejenosti, zato poskusimo ugoditi njegovim predpostavkam. Definirajmo množico $D_+ := \{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}$. Hitro vidimo, da D_+ ni prazna, saj lahko izberemo $x = a$ in $y = b$ in tako vidimo, da D_+ gotovo vsebuje element $a^2 + b^2$. Očitno je množica D_+ podmnožica naravnih števil. Po načelu dobre urejenosti torej sledi, da ima množica D_+ najmanjši element, označimo ga z d. Preostane še pokazati, da je d res največji skupni delitelj števil a in b. To bomo storili tako, da bomo pokazali, da d res deli obe števili ter da vsi ostali delitelji števil a in b delijo tudi d.

Pokažimo, da $d|a$. Da $d|b$, se pokaže analogno. Ker $d \in D_+$, velja $d = ax + by$ za neki števili $x, y \in \mathbb{Z}$. Če $d \nmid a$, potem po osnovnem izreku o deljenju obstajati števili $q, r \in \mathbb{Z},\ 0 \leq r < d$, da $a = qd + r$. Če sedaj pokažemo, da je $r \in D_+$, bomo prišli v protislovje s tem, da je d najmanjše število v D_+.

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy) \quad \checkmark$$

Naj bo e poljuben delitelj števil a in b. To pomeni, da

$$a = a_1 e,$$
$$b = b_1 e.$$

Sledi $d = ax + by = a_1 ex + b_1 ey = e(a_1 x + b_1 y)$, kar pa po definiciji pomeni $e|d$. □

Opomba: Vsak skupni delitelj števil a in b deli njun največji skupni delitelj (a, b).

Posledica: Naj bo $d = (a, b)$. Potem obstajata števili $x, y \in \mathbb{Z}$, da je $d = ax + by$. Posebej, če sta si a in b tuji, se pravi $d = 1$, potem ima enačba $ax + by = 1$ celoštevilski rešitvi x in y.

Ko preučujemo deljivost, se naravno pojavi vprašanje, ali lahko pod pogojem, da $a|c$ in $b|c$, sklepamo, da $ab|c$. Odgovor je v splošnem ne, kdaj to drži, pa nam pove naslednja trditev:

Trditev 5. *Če števili a in b delita število c ter sta si a in b tuji, potem tudi njun produkt ab deli število c. Drugače:*

$$a|c \wedge b|c \wedge (a, b) = 1 \implies ab|c.$$

Dokaz.

$$a|c \implies c = a_1 a$$
$$b|c \implies c = b_1 b$$

Ker $(a, b) = 1$, nam prejšnja posledica pove, da obstajata $x, y \in \mathbb{Z}$, da $ax + by = 1$. Pomnožimo to enakost s c:

$$\begin{aligned} c &= cax + cby \\ &= b_1 bax + a_1 aby \\ &= ab(b_1 x + a_1 y) \end{aligned}$$

To pa po definiciji pomeni, da $ab|c$. □

Trditev 6. *Če število a deli produkt bc ter sta si a in b tuji, potem število a deli število c. Drugače:*

$$a|bc \wedge (a, b) = 1 \implies a|c.$$

Dokaz.

$$a|bc \implies bc = a_1 a$$

Ker $(a, b) = 1$, obstajata $x, y \in \mathbb{Z}$, da $ax + by = 1$. Pomnožimo to enakost s c:

$$\begin{aligned} c &= cax + cby \\ &= cax + a_1 ay \\ &= a(cx + a_1 y) \end{aligned}$$

To pa po definiciji pomeni, da $a|c$. □

Posledica: Naj bo $p \in \mathbb{P}$ praštevilo. Če p deli bc, potem p deli vsaj eno izmed števil b in c.

Dokaz.

- Če p deli b, potem imata p in b največji skupni deliteli, ki je večji od 1. Ker je p praštevilo, mora ta delitelj biti kar število p.
- Če p ne deli b, potem $(p, b) = 1$ in po zgornji trditvi sledi, da p deli c.

□

4 Diofantske enačbe

5 Multiplikativne funkcije

6 Kongruence

6.1 Definicija in osnovne lastnosti

Definicija 10. *Naj bosta $a, b \in \mathbb{Z}$ in naj bo $n \in \mathbb{N}$. Ekvivalenčno relacijo kongruence $\equiv$ po modulu n definiramo na sledeč način:*

$$a \equiv b \pmod{n} \iff n|(a - b).$$

Rečemo, da sta si števili a in b ***kongruentni po modulu*** *n.*

Opomba: Števili a in b sta si kongruentni po modulu n natanko tedaj, ko imata enak ostanek pri deljenju z n.

Ker je relacija kongruence ekvivalenčna, pri fiksnem številu n množica $\mathbb{Z}$ razpade na ekvivalenčne razrede, ki jim pravimo **kongruenčni razredi**. Kvocientno množico $\mathbb{Z}/_{\equiv}$ označimo z $\mathbb{Z}_n$,

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

Posamezne ekvivalenčne razrede $[k]$ nato kar identificiramo z njihovimi predstavniki $k,\ 1 \leq k \leq n-1$, in pišemo

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

Tako izbranim predstavnikom pravimo **standardni predstavniki kongruenčnih razredov**.

Na $\mathbb{Z}_n$ definiramo seštevanje po modulu n in množenje po modulu n kot običajno seštevanje in množenje v $\mathbb{Z}$, pri čemer dobljeni rezultat zamenjamo s standardnim predstavnikom njegovega kongruenčnega razreda. Hitro lahko preverimo, da sta taki operaciji dobro definirani. Za ti operaciji seštevanja in množenja po modulu n postane množica $\mathbb{Z}_n$ grupa za seštevanje in celo kolobar, ki pa v splošnem ni obseg.

Opomba: Kolobar $\mathbb{Z}_n$ je obseg natanko tedaj, ko je n praštevilo.

Trditev 7. *Če velja* $a \equiv b \pmod{n}$ *in* $c \equiv d \pmod{n}$*, potem velja*

1. $a + c \equiv b + d \pmod{n}$
2. $a \cdot c \equiv b \cdot d \pmod{n}$
3. $a^m \equiv b^m \pmod{n}$ *za vsak* $m \in \mathbb{N}$

Dokaz. Iz $a \equiv b \pmod{n}$ sledi $a = b + kn$, prav tako iz $c \equiv d \pmod{n}$ sledi $c = d + ln$. Velja torej

1. $a + c = b + kn + d + ln = b + d + (k + l)n \equiv b + d \pmod{n}$
2. $a \cdot c = (b + kn)(d + ln) = b \cdot d + (bl + dk + kln)n \equiv b \cdot d \pmod{n}$
3. $a^m = (b + kn)^m = b^m + \binom{m}{1} b^{m-1} kn + \cdots + \binom{m}{m-1} b(kn)^{m-1} + (kn)^m = b^m + nk(\ldots) \equiv b^m \pmod{n}$

□

Trditev 8. *Veljajo naslednje trditve:*

1. $a \equiv b \pmod{n}$ *in* $d \mid n \implies a \equiv b \pmod{d}$
2. $a \equiv b \pmod{n_i},\ i = 1, 2, \ldots k$ *in* n_i *so si paroma tuji* $\implies a \equiv b \pmod{\prod_{i=1}^{k} n_i}$
3. $ac \equiv bc \pmod{n} \implies a \equiv b \pmod{\frac{n}{d}}$, *kjer* $d = (c, n)$

Dokaz. 1. Po predpostavki velja $a = b + kn$ in $n = d \cdot l$ za neka $k, l \in \mathbb{Z}$. Sledi $a = b + kld$, kar je ekvivalentno želenemu rezultatu, $a \equiv b \pmod{d}$.

2. Po predpostavki za vsak $i = 1, 2, \ldots k$ velja $n_i \mid a - b$. Ker so si števila n_i paroma tuja, sledi, da tudi njihov produkt deli razliko $a - b$, $\prod_{i=1}^{k} n_i \mid a - b$.

3. Po predpostavki velja $ac = bc + kn$ za neki $k \in \mathbb{Z}$. Ker je d največji skupni delitelj števil c in n, ju lahko zapišemo kot $c = c_1 d$ in $n = n_1 d$. Če to vstavimo v prejšnji izraz, dobimo

$$\begin{aligned} ac_1 d &= bc_1 d + kn_1 d \quad / : d \\ ac_1 &= bc_1 + kn_1 \end{aligned}$$

Velja torej $(a - b)c_1 = kn_1$, od koder sledi $c_1 \mid kn_1$. Vemo pa, da $(c_1, n_1) = 1$, saj je bil d največji skupni delitelj števil c in n. Lahko torej sklepamo, da $c_1 \mid k$ oz. $k = lc_1$ za neki $l \in \mathbb{Z}$. Od tod sledi

$$\begin{aligned} (a - b)c_1 &= lc_1 n_1 \quad / : c_1 \\ a - b &= ln_1 \end{aligned}$$

Vidimo, da $n_1 \mid a - b$, kar je po definiciji ekvivalentno želenemu rezultatu, $a \equiv b \pmod{n_1}$, $n_1 = \frac{n}{d}$.

□

Trditev 9. *Naj bo* $f(x) = \sum_{i=0}^{k} c_i x^i$, $c_i \in \mathbb{Z}$. *Če za* $a, b \in \mathbb{Z}$ *velja* $a \equiv b \pmod{n}$, *potem je* $f(a) \equiv f(b) \pmod{n}$.

Dokaz. Po predpostavki velja $a \equiv b \pmod{n}$. Po 3. točki trditve 8 vemo, da zato velja tudi $a^i \equiv b^i \pmod{n}$, od koder sledi $c_i a^i \equiv c_i b^i \pmod{n}$. Če te člene sedaj seštejemo, dobimo

$$\sum_{i=0}^{k} c_i a^i \equiv \sum_{i=0}^{k} c_i b^i \pmod{n},$$

kar smo želeli pokazati. □

6.2 Kriteriji za deljivost

En izmed primerov uporabe kongruenc je določanje kriterijev za deljivost z določenimi števili. Navedli in dokazali bomo kriterije za deljivost s števili 3, 9, 11 in 7, na enak način pa bi lahko izpelajli kriterije za deljivost s poljubnimi naravnimi števili.

Trditev 10. *Naj bo $n = \sum_{i=0}^{k} c_i 10^i$ desetiški zapis števila $n \in \mathbb{N}$. Označimo s s, t in w sledeče izraze:*

$$s = \sum_{i=0}^{k} c_i$$
$$t = \sum_{i=0}^{k} (-1)^i c_i$$
$$w = c_0 + 3c_1 + 2c_2 - c_3 - 3c_4 - 2c_5 + c_6 + 3c_7 + \ldots$$

Potem velja:

(*i*) $3 \mid n \iff 3 \mid s$ *(in* $n \equiv s \pmod 3$*)*

(*ii*) $9 \mid n \iff 9 \mid s$ *(in* $n \equiv s \pmod 9$*)*

(*iii*) $11 \mid n \iff 11 \mid t$ *(in* $n \equiv t \pmod{11}$*)*

(*iv*) $7 \mid n \iff 7 \mid w$ *(in* $n \equiv w \pmod 7$*)*

Dokaz. (*i*) $10 \equiv 1 \pmod 3 \implies 10^i \equiv 1 \pmod 3$

$$n = \sum_{i=0}^{k} c_i 10^i \equiv \sum_{i=0}^{k} c_i 1 = s \pmod 3 \quad \checkmark$$

(*ii*) $10 \equiv 1 \pmod 9 \implies 10^i \equiv 1 \pmod 9$

$$n = \sum_{i=0}^{k} c_i 10^i \equiv \sum_{i=0}^{k} c_i 1 = s \pmod 9 \quad \checkmark$$

(*iii*) $10 = -1 \pmod{11} \implies 10^i \equiv (-1)^i \pmod{11}$

$$n = \sum_{i=0}^{k} c_i 10^i \equiv \sum_{i=0}^{k} (-1)^i c_i = t \pmod{11} \quad \checkmark$$

(*iv*) $10 \equiv 3 \pmod 7$, $10^2 \equiv 9 \equiv 2 \pmod 7$, $10^3 = 10 \cdot 10^2 \equiv 6 \equiv -1 \pmod 7$
$10^4 = 10^2 \cdot 10^2 \equiv -3 \pmod 7$, $10^5 = 10^2 \cdot 10^3 \equiv -2 \pmod 7$, $\ldots$
Opazimo vzorec, pa katerem se nadaljuje zaporedje. Zapišemo lahko torej

$$n = c_0 + c_1 10 + c_2 10^2 + c_3 10^3 + c_4 10^4 + c_5 10^5 + c_6 10^6 + c_7 10^7 + \ldots \equiv$$
$$\equiv c_0 + 3c_1 + 2c_2 - c_3 - 3c_4 - 2c_5 + c_6 + 3c_7 + \ldots = w \pmod 7 \quad \checkmark$$

□

6.3 Reducirani sistem ostankov

Definicija 11. ***Reducirani sistem ostankov*** *po modulu $n \in \mathbb{N}$ tvorijo predstavniki tistih kongruenčnih razredov, ki so si tuji z modulom n.* ***Standardni reducirani sistem ostankov*** *označimo z $\mathbb{Z}_n^\times \subseteq \mathbb{Z}_n$ in ga sestavljajo števila med 1 in n, ki so tuja n.*
Moč množice $\mathbb{Z}_n^\times$ označimo s $\phi(n) = |\mathbb{Z}_n^\times|$. Funkcija ϕ se imenuje ***Eulerjeva funkcija****.*

Primer: Če je $p \in \mathbb{P}$, je $\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}$ in $\phi(p) = p - 1$.

Trditev 11. *1. Naj bo $\{r_1, r_2, \ldots, r_n\}$ neki popolni sistem ostankov* (mod n). *Če velja $a, b \in \mathbb{Z}$ in $(a, n) = 1$, potem je tudi $\{ar_1+b, ar_2+b, \ldots, ar_n+b\}$ popolni sistem ostankov* (mod n).

2. Naj bo $\{q_1, q_2, \ldots, q_{\phi(n)}\}$ neki reducirani sistem ostankov (mod n). *Če je $a \in \mathbb{Z}$ in $(a, n) = 1$, potem je tudi $\{aq_1, aq_2, \ldots, aq_{\phi(n)}\}$ reducirani sistem ostankov* (mod n).

Dokaz. 1. Zadošča pokazati, da nobeni dve števili v drugi množici nista kongruentni po modulu n.
Predpostavimo $ar_i + b \equiv ar_j + b \pmod{n}$ za neka $i, j = 1, 2, \ldots, n$. Sledi $ar_i \equiv ar_j \pmod{n}$. Ker $(a, n) = 1$, lahko iz tega sklepamo, da $r_i \equiv r_j \pmod{n}$. Ker sta r_i in r_j elementa popolnega sistema ostankov, morata zato biti kar enaka. Velja torej tudi $i = j$, kar pomeni, da je vsako število $ar_i + b$ kongruentno po modulu n le samemu sebi.

2. Iz 1. točke izreka že vemo, da so si elementi q_i paroma nekongruentni. Razmisliti še moramo, da so si res vsi tuji z n. Število q_i si je tuje z n, saj je element reduciranega sistema ostankov, a pa si je tuj z n po predpostavki. Sledi, da si je tudi produkt aq_i tuj z n.

□

6.4 Rešljivost linearih kongruenc

Izrek 5 (o rešljivosti linearnih kongruenc)**.** *Za linearno kongruenco $ax \equiv b$* (mod n) *velja:*

1. če je $(a, n) = 1$, ima linearna kongruenca natanko eno rešitev po modulu n,

2. če je $d = (a, n) > 1$ in $d \nmid b$, linearna kongruenca nima rešitev,

3. *če je* $d = (a, n) > 1$ *in* $d \mid b$*, ima linearna kongruenca* d *nekongruentnih rešitev po modulu* n*. Te rešitve so oblike*

$$x_0 + k\frac{n}{d} \pmod{n},\ k = 0, 1, 2, \ldots, d-1,$$

kjer je x_0 *rešitev kongruence* $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

Posledica: $\mathbb{Z}_n^\times$ je grupa za množenje, saj ima enačba $ax \equiv 1 \pmod{n}$ natanko eno rešitev za a, ki je tuj n.

Dokaz. 1. Velja $(a, n) = 1$, zato, ko x preteče vse kongruenčne razrede (mod n) natanko enkrat, tudi element ax preteče vse kongruenčne razrede natanko enkrat.

2. Po predpostavki velja $d = (a, n) > 1$, zato lahko a in n zapišemo kot $a = a_1 d$ in $n = n_1 d$. Denimo, da obstaja rešitev $ax \equiv b \pmod{n}$ dane linearne kongruence. Velja torej $a = b + kn$ za neki $k \in \mathbb{Z}$. Sledi sklep

$$a_1 dx = b + kn_1 d \implies d(a_1 x - kn_1) = b \implies d \mid b,$$

kar pa je v protislovju z drugo predpostavko.

3. Po predpostavki velja $d \mid b$, zato lahko izraz $ax \equiv b \pmod{n}$ delimo z d in dobimo $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$, pri čemer velja $(\frac{a}{d}, \frac{b}{d}) = 1$. Po 1. točki izreka sledi, da obstaja natanko ena rešitev x_0 te kongruence po modulu $\frac{n}{d}$. Velja torej $\frac{a}{d}x_0 = \frac{b}{d} + k\frac{n}{d}$ za neki $k \in \mathbb{Z}$, od koder očitno sledi, da je x_0 rešitev dane kongruence tudi po modulu n. Vidimo pa, da kongruenco po modulu $\frac{n}{d}$ reši tudi $x_k = x_0 + k\frac{n}{d}$ in zato reši tudi kongruenco po modulu n. Naj omenim, da je rešitev po modulu $\frac{n}{d}$ res ena sama, saj so si vsi x_k kongruentni modulo $\frac{n}{d}$, vendar ne modulo n. Če x_k zapišemo nekoliko drugače, $x_k = x_0 + n\frac{k}{d}$, je lažje opaziti, da je število do kongruence po modulu n različnih x_k ravno d, in sicer za $k \in \{0, 1, 2, \ldots, d-1\}$ (kjer pri $k = 0$ dobimo kar x_0).

□

Opomba: Isti rezultat lahko izpeljemo iz izreka o rešljivosti linearnih diofantskih enačb.

Opomba: Presenetljivo ima linearna enačba $ax \equiv b \pmod{n}$ lahko več rešitev. To se nad $\mathbb{R}$ ali $\mathbb{C}$ ne zgodi. Razlog je v tem, da ima $\mathbb{Z}_n$ v splošnem delitelje niča.

$$\frac{n}{d},\ d \in \mathbb{Z}_n \setminus \{0\},\ \frac{n}{d} \cdot d = n \equiv 0 \pmod{n}$$

6.5 Sistemi linearnih kongruenc

Iščemo $x \in \mathbb{Z}$, ki reši sistem:

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{n_1} \\ a_2 x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ a_k x &\equiv b_k \pmod{n_k} \end{aligned}$$

Potrebni pogoj za rešljivost celotnega sistema je seveda ta, da je rešljiva vsaka posamezna kongruenca v sistemu. Iz izreka o rešljivosti linearnih kongruenc vemo, da ima linearna kongruenca lahko eno ali več rešitev, lahko pa ni rešljiva. Denimo, da so rešljive vse kongruence v sistemu in izberimo po eno rešitev za vsako.

$$x \equiv c_1 \pmod{n_1},\ x \equiv c_1 \pmod{n_1},\ \cdots,\ x \equiv c_1 \pmod{n_1}$$

Posebej si bomo ogledali primer sistema dveh linearnih kongruenc:

$$\begin{aligned} x &\equiv c_1 \pmod{n_1} \\ x &\equiv c_2 \pmod{n_2} \end{aligned}$$

Problem reševanja linearnih kongruenc bomo prevedli na problem reševanja diofantskih enačb. Iz prve enačbe sistema tako dobimo diofantsko enačbo $x = c_1 + kn_1,\ k \in \mathbb{Z}$, ki jo vstavimo v drugo kongruenco:

$$\begin{aligned} c_1 + kn_1 &\equiv c_2 \pmod{n_2} \\ kn_1 &\equiv c_2 - c_1 \pmod{n_2} \end{aligned}$$

Izrek o rešljivosti linearnih kongruenc nam o zgornji kongruenci pove naslednje:

- če je $(n_1, n_2) = 1$, ima kongruenca natanko eno rešitev
- če je $(n_1, n_2) = d > 1$, je kongruenca rešljiva natanko tedaj, ko velja $c_1 \equiv c_2 \pmod{d}$ in tedaj ima natanko d rešitev

Lahko torej sklepamo, da je rešitev, če obstaja, določena modulo $n_1 \cdot n_2$ (do večkratnikov rešitev). ???

Opomba: Za sistem z več kongruencami lahko zaporedoma uporabljamo zgornjo metodo na dveh.

Primer: Nace pove Mojci, da ima manj kot 100 bonbonov. Ker je Mojca sladkosneda, je sprva razočarana, vendar jo čez čas le začne begati, koliko bonbonov ima Nace. Ko ga vpraša, ji Nace enigmatično odvrne, da mu ostane eden, če jih zloži v kupčke po 4, če jih zloži v kupčke po 6, mu ostanejo trije, če jih zloži v kupčke po 7, pa mu jih ostane pet. Ali lahko Mojca ugotovi, koliko bonbonov ima Nace?

Dane podatke najprej zapišemo s kongruencami in dobimo sledeč sistem:

$$\begin{aligned} n &\equiv 1 \pmod 4 \\ n &\equiv 3 \pmod 6 \\ n &\equiv 5 \pmod 7 \end{aligned}$$

Iz prve kongruence dobimo diofantsko enačbo $n = 1 + 4k$, ki jo vstavimo v drugo kongruenco. Sledi

$$\begin{aligned} 1 + 4k &\equiv 3 \pmod 6 \\ 4k &\equiv 2 \pmod 3 \quad / : 2 \\ 2k &\equiv 1 \pmod 3 \quad / \cdot 2 \qquad (*) \\ 4k \equiv k &\equiv 2 \pmod 3 \end{aligned}$$

V vrstici $(*)$ smo se želeli znebiti koeficienta 2 pred k. Pri tem se je dobro zavedati, da smo zato kongruenco pomnožili z inverzom števila 2 v kolobarju $\mathbb{Z}_3$, ki je kar število 2 samo.
Iz dobljene kongruence sledi $k = 2+3l$ za neki $l \in \mathbb{Z}$. Velja torej $n = 1+4k = 9 + 12l$, kar je po definiciji ekvivalentno izrazu $n \equiv 9 \pmod{12}$, ki je rešitev prvih dveh kongruenc sistema. Zdi se, da ena rešitev manjka, saj je največji skupni delitelj modulov $(4, 6) = 2$ in bi zato morali imeti dve rešitvi, vendar to bi držalo za rešitve po modulu 24. Tako bi dobili rešitvi $n_1 \equiv 9 \pmod{24}$ in $n_2 \equiv 21 \pmod{24}$, ki pa sta po modulu 12 kongruentni in sta hkrati zajeti v izrazu $n \equiv 9 \pmod{12}$. Vidimo torej, da gre le za drugačen, ekvivalentni zapis rešitve. Ta rezultat vstavimo v tretjo kongruenco in dobimo:

$$\begin{aligned} 9 + 12l &\equiv 5 \pmod 7 \\ 12l &\equiv -4 \equiv 3 \pmod 7 \end{aligned}$$

Da ilustriramo raznolikost reševanja problemov te narave in pokažemo nekaj izmed pristopov, se bomo do končnega rezultata prikopali na dva različna načina.

1.

$$\begin{aligned} 12l &\equiv 3 \pmod 7 \quad / : 3 && \text{delimo} \\ 4l &\equiv 1 \pmod 7 \quad / \cdot 2 && \text{množimo z inverzom} \\ l &\equiv 2 \pmod 7 \end{aligned}$$

2.

$$\begin{aligned} 12l &\equiv 3 \pmod 7 && 7l \equiv 0 \pmod 7 \\ 5l &\equiv 3 \pmod 7 \quad / \cdot (-1) && \text{množimo} \\ -5l &\equiv -3 \pmod 7 && -5l \equiv 2l,\ -3 \equiv 4 \pmod 7 \\ 2l &\equiv 4 \pmod 7 \quad / : 2 && \text{delimo} \\ l &\equiv 2 \pmod 7 \end{aligned}$$

Po obeh poteh smo prišli do rezultata $l = 2 + 7m$. Končni rezultat je torej

$$n = 9 + 12(2 + 7m) = 33 + 84m,\ m \in \mathbb{Z}.$$

Rešitev sistema je kongruenca $n \equiv 33 \pmod{84}$, ki nam poda kongruenčni razred, v katerem se mora nahajati n, da bo rešil dani sistem linearnih kongruenc (tudi tukaj je na mestu prejšnji komentar o eni sami rešitvi namesto dveh). Nas seveda zanimajo le nekateri predstavniki tega ekvivalenčnega razreda, in sicer tisti, ki ležijo med 1 in 99. V tem primeru je tak le eden, število 33. Nace ima torej 33 bonbonov, odgovor na naše vprašanje pa se glasi, da Mojca lahko ugotovi, koliko bonbonov ima Nace (če je le pridno poslušala pri predavanjih ETŠ).

V primeru, ko so si moduli paroma tuji, pa vedno obstaja natanko ena rešitev sistema $x \equiv c_i$ za $i = 1, 2, \ldots, k$ po modulu $n = \prod_{i=1}^{k} n_i$. To nam pove naslednji izrek:

Izrek 6 (kitajski izrek o ostankih)**.** *Sistem linearnih kongruenc $x \equiv c_i \pmod{n_i}$ za $i = 1, 2, \ldots, k$, kjer so si moduli n_i paroma tuji, ima natanko eno rešitev po modulu $N := \prod_{i=1}^{k} n_i$. Rešitev je podana s formulo*

$$x \equiv \sum_{i=1}^{k} c_i N_i k_i \pmod N,$$

kjer je $N_i = \frac{N}{n_i}$ in $N_i k_i \equiv 1 \pmod{n_i}$.

Dokaz. Naj si bodo naravna števila $n_i,\ i = 1, 2, \ldots, k$, paroma tuja. Razmislimo najprej, da ima sistem $x \equiv c_i \pmod{n_i}$ natanko eno rešitev. Oglejmo si

podsistem kongruenc $x \equiv c_1 \pmod{n_1}$ in $x \equiv c_2 \pmod{n_2}$. Po predpostavki izreka sta si modula n_1 in n_2 tuja. Vemo torej, da ima ta podsistem natanko eno rešitev d_1 po modulu $n_1 \cdot n_2$. Sedaj si oglejmo sistem kongruenc $x \equiv d_1 \pmod{n_1 n_2}$ in $x \equiv c_3 \pmod{n_3}$. Ker velja $(n_1, n_3) = 1$ in $(n_2, n_3) = 1$, velja tudi $(n_1 n_2, n_3) = 1$. Spet lahko sklepamo, da ima sistem teh dveh kongruenc natanko eno rešitev d_2 po modulu $n_1 \cdot n_2 \cdot n_3$. Analogno poiščemo rešitev sistema kongruenc $x \equiv d_2 \pmod{n_1 n_2 n_3}$ in $x \equiv c_4 \pmod{n_4}$, ki je spet natanko ena. Postopek ponavljamo, dokler ne pridemo do rešitve d_{k-1} po modulu $N := \prod_{i=1}^{k} n_i$ celotnega sistema, za katero vemo, da je natanko ena. Reševanje celotnega sistema i kongruenc smo tako le prevedli na reševanje sistema dveh kongruenc, kot smo to naredili v zgornjem primeru za sistem treh kongruenc.

Preostane še pokazati, da velja $d_{k-1} \equiv \sum_{i=1}^{k} c_i N_i k_i \pmod{N}$. Dovolj je kar preveriti, da je $x \equiv \sum_{i=1}^{k} c_i N_i k_i \pmod{N}$ res rešitev našega sistema $x \equiv c_i \pmod{n_i}$. Po prvi točki trditve 8 sledi, da velja $x \equiv \sum_{i=1}^{k} c_i N_i k_i \pmod{n_i}$ za vse i, saj n_i deli N za vse i. Po predpostavki izreka dodatno velja $N_i = \frac{N}{n_i}$ in $N_i k_i \equiv 1 \pmod{n_i}$. Če sumand $c_i N_i k_i$ zapišemo kot $c_i \frac{N}{n_i} k_i$, je lažje opaziti, da velja

$$c_i \frac{N}{n_i} k_i \pmod{n_j} \equiv \begin{cases} c_i & ;\ i = j \\ 0 & ;\ i \neq j \end{cases}$$

Od tod sledi, da za vsak $i \in \{1, 2, \ldots, k\}$ res velja

$$x \equiv \sum_{i=1}^{k} c_i N_i k_i \equiv c_i \pmod{n_i}.$$

□

6.6 Eulerjeva funkcija ϕ

Eulerjevo funkcijo ϕ smo omenili že pri definiciji reduciranega sistema ostankov. Formalno je definirana kot

$$\phi(n) := \begin{cases} 1 & ;\ n = 1 \\ |\mathbb{Z}_n^\times| & ;\ n \geq 2 \end{cases}$$

Lema 1 (Gauß)**.** *Za vsak $n \in \mathbb{N}$ velja*

$$\sum_{d|n} \phi(d) = n.$$

Dokaz. Za vsak $d,\ d \mid n$, definirajmo množico

$$A_d := \{k \in \mathbb{Z}_n \mid (k, n) = d\}.$$

Pri tem kot elemente $\mathbb{Z}_n$ razumemo standardne prestavnike kongruenčnih razredov. Za vsak element k tako definirane množice A_d velja $k = k_1 d$ za neki k_1 in posledično $(k_1, \frac{n}{d}) = 1$. Števila k_1 so ravno vsa števila, tuja modulu $\frac{n}{d}$, zato tvorijo reducirani sistem ostankov $\mathbb{Z}_{\frac{n}{d}}^{\times}$. Število različnih k_1 je enako številu različnih k, se pravi moči množice A_d, torej velja

$$|A_d| = \phi(\frac{n}{d}).$$

Ker so množice A_d paroma disjunktne, tvorijo razbitje množice $\mathbb{Z}_n$. Od tod sledi, da je moč množice $\mathbb{Z}_n$ kar enaka vsoti moči vseh množic A_d:

$$n = |\mathbb{Z}_n| = \sum_{d|n} A_d = \sum_{d|n} \phi(\frac{n}{d}) = \sum_{d|n} \phi(d)$$

□

Posledica:

1. Funkcija ϕ je multiplikativna.
2. $\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} \implies \phi(p^\alpha) = p^\alpha(1 - \frac{1}{p})$
3. Če je $n = \prod_{i=1}^{k} p_i^{s_i}$, je $\phi(n) = n \prod_{i=1}^{k}(1 - \frac{1}{p_i})$.

Dokaz.

1. Sledi iz Gaußove leme, saj je $g(n) = n$ multiplikativna.
2. Sledi iz Gaußove leme z uporabo Möbiusove inverzne formule:

$$\phi(p^\alpha) = \sum_{d|p^\alpha} \mu(d)\frac{p^\alpha}{d} = \mu(1)\frac{p^\alpha}{1} + \mu(p)\frac{p^\alpha}{p} = p^\alpha(1 - \frac{1}{p}),$$

   pri čemer smo upoštevali $\mu(1) = 1$ in $\mu(p) = -1$.

3. ???

□

Množica $\mathbb{Z}_n$ je grupa za seštevanje, množica $\mathbb{Z}_n^{\times}$ pa je grupa za množenje. Inverz v grupi $\mathbb{Z}_n^{\times}$ lahko izračunamo s pomočjo Eulerjevega izreka:

Izrek 7 (Euler)**.** *Naj bo $n \in \mathbb{N}$ in $a \in \mathbb{Z}$. Če sta si števili a in n tuji, $(a, n) = 1$, velja*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Dokaz. Naj bo $\{q_1, q_2, \ldots, q_{\phi(n)}\}$ reducirani sistem ostankov po modulu n. Po predpostavki velja $(a, n) = 1$, zato po drugi točki trditve 11 sledi, da je tudi $\{aq_1, aq_2, \ldots, aq_{\phi(n)}\}$ reducirani sistem ostankov po modulu n. Ker sta obe množici reducirana sistema ostankov po modulu n, vsebujeta do kongruence po modulu n enake elemente. Izjava $q_i \equiv aq_i \pmod{n}$ nujno ne velja, gotovo pa velja

$$\prod_{i=1}^{\phi(n)} q_i \equiv \prod_{i=1}^{\phi(n)} aq_i \equiv a^{\phi(n)} \prod_{i=1}^{\phi(n)} q_i \pmod{n}.$$

V zgornji enačbi lahko pokrajšamo $\prod_{i=1}^{\phi(n)} q_i$ in dobimo rezultat

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

□

Posledica: Naj bo p praštevilo in $a \in \mathbb{Z}$. Če p ne deli a, $p \nmid a$, velja

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ta izrek se imenuje *mali Fermatov izrek*.

Primer: S pomočjo Eulerjevega izreka bomo rešili kongruenco

$$x^9 \equiv 5 \pmod{33}.$$

Za $n = 33 = 3 \cdot 11$ zaradi multiplikativnost ϕ velja $\phi(n) = \phi(3) \cdot \phi(11)$. Ker sta 3 in 11 praštevili, velja $\phi(3) = 2$ in $\phi(11) = 10$, od koder sledi $\phi(n) = 20$. Po Eulerjevem izreku torej velja

$$a^{20} \equiv 1 \pmod{33}$$

za neki a, ki je tuj 33. Ker je $(5, 33) = 1$ in je x^9 kongruenten 5 po modulu 33, sta si tudi števili x in 33 tuji, $(x, 33) = 1$. S pomočjo Eulerjevega izreka se bomo poskusili znebiti potence nad x. Velja $(9, 20) = 1$, zato obstajata taki števili $u, v \in \mathbb{Z}$, da velja $9u + 20v = 1$ oz. $9u = 1 - 20v$. Opazimo, da je tak par celih števil npr. par $u = 9$ in $v = -4$, saj $9 \cdot 9 = 81 = 1 - (-4) \cdot 20$. Sledi

$$\begin{aligned} x^9 &\equiv 5 \pmod{33} \quad /^9 \\ x^{81} &\equiv 5^9 \pmod{33} \\ x^{81} &= x^{1+4\cdot 20} = x \cdot (x^{20})^4 \equiv x \cdot 1^4 \equiv x \pmod{33} \end{aligned}$$

Vemo torej, da $x \equiv 5^9 \pmod{33}$. Potence te vrste se da pogosto precej poenostaviti z redukcijo po modulu. V tem primeru bi izraz najbrž hitreje izračunali kar "na roke" kot $5 \cdot 625^2$, vendar bomo način z redukcijo po modulu iz pedagoških razlogov vseeno demonstrirali.

$$\begin{aligned}
5^2 &= 25 \equiv -8 \pmod{33} \\
5^3 &\equiv -8 \cdot 5 = -40 \equiv -7 \pmod{33} \\
5^6 &= (5^3)^2 \equiv 49 \equiv 16 \pmod{33} \\
5^9 &= 5^6 \cdot 5^3 \equiv -7 \cdot 16 = -112 \equiv -13 \equiv 20 \pmod{33}
\end{aligned}$$

Rešitev kongruence je torej $x \equiv 20 \pmod{33}$.

6.7 Polinomske kongruence

Naj bo f polinom z celimi koeficienti, ki je stopnje s modulo $n \in \mathbb{N}$. Po definiciji to pomeni, da je koeficient pri x^s modulo n različen od 0, koeficienti pri vsej višjih členih pa so kongruentni 0 modulo n. Iščemo rešitev kongruence

$$f(x) \equiv 0 \pmod{n}.$$

Iz prve in druge točke trditve 8 in kitajskega izreka o ostankih, lahko o rešitvah take kongruence sklepamo naslednje:

- Če je $n = \prod_{i=1}^{k} n_i$, kjer so n_i tuja si števila, nam x, za katerega velja $f(x) \equiv 0 \pmod{n}$, da rešitve za kongruenc $f(x) \equiv 0 \pmod{n_i}$ za $i = 1, 2, \ldots, k$.
- Če so a_i rešitve kongruenc $f(x) \equiv 0 \pmod{n_i}$ za $i = 1, 2, \ldots, k$, potem ima sistem kongruenc $x \equiv a_i \pmod{n_i}$ natanko eno rešitev x modulo n in ta reši kongruenco $f(x) \equiv 0 \mod n$.

Sklepamo, da je za reševanje kongruence $f(x) \equiv 0 \pmod{n}$ torej dovolj poznati rešitve kongruenc $f(x) \equiv 0 \pmod{p_i^{r_i}}$, kjer je $n = \prod_{i=1}^{k} p_i^{r_i}$ enolična faktorizacija. Pri tem je prvi korak iskanje rešitev modulo p, $p \in \mathbb{P}$.

Za običajne polinome nad $\mathbb{Z}$ velja, da imajo lahko največ toliko ničel, kolikor je stopnja polinoma. Ker nas zanima, koliko rešitev lahko pričakujemo za našo polinomsko kongruenco, se naravno pojavi vprašanje, ali kaj podobnega velja tudi za polinome nad $\mathbb{Z}_n$. Oglejmo si naslednji primer:

Primer: Poišči rešitve polinomske kongruence

$$x^2 \equiv 1 \pmod{15}.$$

Že v $\mathbb{Z}$ za dano kongruenco najdemo dve rešitvi, in sicer $x_1 = 1$ ter $x_2 = -1$. Ni težko ugotoviti, da pa sta rešitvi tudi $x_3 = 4$ ter $x_4 = -4$. Rutinsko lahko preverimo, da so to res vse rešitve. Tako smo dobili štiri rešitve za enačbo druge stopnje. Da bi ta rezultat lažje razumeli, zapišimo našo kongruenco nekoliko drugače:

$$x^2 \equiv 1 \pmod{15} \iff (x-1)(x+1) \equiv 0 \pmod{15}$$

Tako bi se reševanja običajne polinomske enačbe formalno lotili tudi v $\mathbb{Z}$. Ker mora biti vsaj eden izmed faktorjev enak 0, bi dobili rešitvi $x_1 = 1$ ter $x_2 = -1$. Ta sklep pa velja le, ker kolobar $\mathbb{Z}$ nima deliteljev niča, kar v $\mathbb{Z}_n$ v splošnem ne velja. Zato dobimo tu dve dodatni rešitvi, saj sta v kolobarju $\mathbb{Z}_{15}$ števili 3 in 5 delitelja niča.

O številu rešitev polinomskih kongruenc nam več pove naslednji izrek:

Izrek 8 (Lagrange)**.** *Naj bo f polinom s koeficienti v $\mathbb{Z}$ in $p \in \mathbb{P}$. Če ima polinom f stopnjo s modulo p, potem ima kongruenca $f(x) \equiv 0 \pmod{p}$ največ s rešitev modulo p.*

Dokaz. Lagrangeev izrek bomo dokazali z indukcijo po s.

$s = 1$: $f(x) \equiv a_1 x + a_0 \pmod{p}$. Ker je stopnja $s = 1$, velja $a_1 \not\equiv 0$. Sledi $(a_1, p) = 1$, zato ima kongruenca po prejšnjih sklepih res natanko eno rešitev. ✓

$s \to s+1$: $f(x) \equiv a_{s+1}x^{s+1} + \cdots + a_0 \pmod{p}$. Enako kot zgoraj velja $a_{s+1} \not\equiv 0 \pmod{p}$. Denimo, da ima f več kot $s+1$ ničel c_i modulo p, $i = 1, 2, \ldots, s+2$.

$$Ničle različne???????$$

□

7 Kriptografija

V tem razdelku bomo spoznali, kako lahko uporabimo teorijo števil za skrivanje sporočil. Naš namen bo sporočilo spremeniti tako, da ga nihče brez dodatnih iniformacij ne bo znal prebrati.

7.1 Afina šifra

Ideja je, da izberemo novo abecedo in preslikavo iz prvotne abecede v novo. To bomo naredili tako, da bomo vzeli neko permutacijo znakov. Če črke slovenske abecede oštevilčimo, dobimo bijektivno korespondenco med črkami

abecede (teh je 25) in pa elementi grupe $\mathbb{Z}_{25}$. Tako moramo izbrati samo še preslikavo $f : \mathbb{Z}_{25} \to \mathbb{Z}_{25}$. Ta preslikava mora biti bijektivna, saj v nasprotnem primeru besedila ne bi mogli dešifrirati. Najbolj preprost primer take preslikave je kar afina preslikava

$$f(x) \equiv ax + b \pmod{25},$$

kjer $(a, 5) = 1$. Njena inverzna preslikava f^{-1} je podana s predpisom

$$f^{-1}(y) \equiv a^{-1}(y - b) \pmod{25}.$$

Primer: Cezarjeva šifra je bila pomik abecede za tri znake, $x \mapsto x + 3$.

Ta metoda ima seveda nekaj pomanjkljivosti. Ena je ta, da smo ohranili presledke med besedami in ločila, toda to z lahkoto odpravimo tako, da jih dodamo kot nove znake v našo abecedo. Glavna slabost te metode je pa ta, da lahko za daljša besedila ugotovimo šifro na podlagi zastopanosti posameznih črk, če le vemo, v katerem jeziku je osnovno besedilo.

Tabela 1: Zastopanost črk v slovenski abecedi

Črka	**%**	**Črka**	**%**	**Črka**	**%**	**Črka**	**%**	**Črka**	**%**
E	10,71%	*L*	5,27%	*V*	3,76%	*Z*	2,10%	*H*	1,05%
A	10,47%	*S*	5,05%	*K*	3,70%	*B*	1,94%	*C*	1,00%
O	9,08%	*R*	5,01%	*D*	3,39%	*U*	1,88%	*Š*	0,66%
I	9,04%	*J*	4,67%	*P*	3,37%	*G*	1,64%	*Ž*	0,65%
N	6,33%	*T*	4,33%	*M*	3,30%	*Č*	1,48%	*F*	0,11%

Pojavi se vprašanje, za koliko znakov moramo poznati vrednost preslikave f, da lahko določimo koeficienta a in b ter s tem preslikavo f. Naj bodo x_0, x_1, y_0 in y_1 znani znaki ter $x_0 \mapsto y_0$, $x_1 \mapsto y_1$. Dobimo sistem dveh kongruenc z dvema neznankama.

$$f(x_0) \equiv ax_0 + b = y_0 \pmod{25}$$
$$f(x_0) \equiv ax_1 + b = y_1 \pmod{25}$$

Iz sistema z eliminacijo neznanke b dobimo kongruenco $a(x_0 - x_1) \equiv y_0 - y_1 \pmod{25}$. Ta enačba bo enolično rešljiva, če bo $x_0 - x_1$ obrnljiv element v $\mathbb{Z}_{25}$. To bo res, ko bo $x_0 - x_1$ tuj modulu 25, torej $x_0 \not\equiv x_1 \pmod{5}$. Če pa velja $x_0 \equiv x_1 \pmod{5}$, dobimo za a pet možnosti. Odgovor se torej glasi, da je odgovor odvisen od znakov, katerih vrednosti poznamo.

Opomba: Metodo afinega šifriranja lahko izboljšamo z uporabo več preslikav.

7.2 Hillova šifra

Hillovo šifriranje vzame idejo afinega šifriranja in jo znatno nadgradi. Znakom (vzemimo tokrat črke slovenske abecede skupaj s presledkom) spet priredimo elemente grupe $\mathbb{Z}_{26}$. Nato sporočilo, ki ga želimo šifrirati, razdelimo na bloke po n znakov, kjer je n povsem poljubno naravno število. Besedilo smo torej razdelili na določeno število n-teric, ki jih bomo v nadaljevanju obravnavali kot vektorje. Namesto afine preslikave sedaj vzamemo naključno obrnljivo linearno preslikavo $A \in \mathbb{Z}_{26}^{n\times n}$ in jo uporabimo na vsakem vektorju posebej:

$$A(c_1, \ldots, c_n) \equiv (b_1, \ldots, b_n) \pmod{26}.$$

Ta metoda je veliko učinkovitejša od afinega šifriranja, saj je sedaj slika vsake črke odvisna tudi od ostalih črk v njeni n-terici, saj se s spremembo ene same črke (komponente vektorja) popolnoma spremeni tudi slika n-terice (vektorja), ki ji črka pripada. Za dešifriranje takega besedila moramo poznati preslikavo A.

Opomba: Če izberemo $n = 1$, je to kar metoda afinega šifriranja pri $b = 0$.

Opomba: Matrika $A \in \mathbb{Z}_{26}^{n\times n}$ je obrnljiva natanko tedaj, ko $detA \not\equiv 0 \pmod{26}$. Povsem poljubna matrika torej ni ustrezna. Število ustreznih matrik lahko povečamo z izbiro praštevilskega modula, kjer bodo ustrezne vse matrike z determinanto različno od 0. V našem primeru lahko to dosežemo npr. tako, da dodamo piko, vejico in vprašaj ter tako dobimo modul 29.

Veliko boljše metode enkripcije so eksponentne šifre (Hellman, 1976, tvorec ideje o javnih ključih).

7.3 Ideja o javnih ključih

Pri tej metodi vsakemu znaku priredimo dvomestno numerično vrednost in jih kot pri Hillovem šifriranju združimo v bloke po n. Če vzamemo npr. $n = 2$:

$$A \mapsto 00, \qquad B \mapsto 01, \qquad \cdots \qquad \check{Z} \mapsto 24, \qquad \_ \mapsto 25,$$

dobimo bloke med 0000 in 2525. V naslednjem koraku vzamemo $2n$-mestno praštevilo, večje od vrednosti v zadnjem bloku. V našem primeru torej vzamemo neko 4-mestno praštevilo $p > 2525$. Nato izberemo še šifrirni ključ $e \in \mathbb{N},\ (e, p-1) = 1$, in sporočilo zašifriramo:

$$y \equiv x^e \pmod{p}.$$

Ker je p praštevilo, je vsak $x \neq 0000$ številu p tuj. Zdaj potrebujemo še inverzno preslikavo $x^e \mapsto x$. Pri tem si bomo pomagali z malim Fermatovim izrekom:

$$x^{p-1} \equiv 1 \pmod{p}.$$

Ker smo e izbrali tako, da $(e, p-1) = 1$, obstajata $a, b \in \mathbb{Z}$, da velja $ae = 1 + b(p-1)$. Sledi:

$$(x^e)^a = x \cdot x^{b(p-1)} \equiv x \pmod{p}$$

Iskana inverzna preslikava je torej potenciranje na potenco a. Označimo $d := a$ in d imenujemo *dešifrirni ključ*.

Če vsi poznamo števili e in p lahko zašifriramo sporočilo in ga pošljemo po javnem kanalu, prebere ga pa lahko le tisti, ki pozna dešifrirni ključ d. Očitna slabost te metode je pa ta, da lahko s poznavanjem e in p ključ d izračunamo, d je namreč inverz števila e po modulu $p-1$. To slabost odpravi algoritem RSA.

7.4 Algoritem RSA

Algoritem RSA (Rivest, Shamir, Adleman, 1977) podobno kot zgoraj namesto praštevilskega modula vzame modul r, ki je produkt dveh velikih praštevil, $r = p \cdot q,\ p \neq q$. Sporočilo zašifriramo kot zgoraj, $x \mapsto y \equiv x^e \pmod{r}$. Z uporabo dešifrirnega ključa d lahko sporočilo dešifriramo, $y \mapsto y^d \equiv (x^e)^d \equiv x \pmod{r}$. Pri tem mora veljati

$$(e, \phi(r)) = 1 \qquad \text{in} \qquad d \cdot e \equiv 1 \pmod{(\phi(r))}.$$

Zdaj brez poznavanja faktorizacije $r = p \cdot q$ iz znanih e in r ne moremo izračunati dešifrirnega ključa d.

Ta metoda med drugim omogoča digitalni podpis. Ker bi z razvojem kvantnih računalnikov ta algoritem postal popolnoma neuporaben, se iščejo alternative.