ELEMENTARNA ARITMETIKA

SLAVKO MOCONJA

Sadržaj

I. Relacija deljivosti.

1. **Definicija.** Relacija deljivosti na skupu $\mathbb{Z}$ definisana je sa $m \mid n$ akko $n = qm$ za neko $q \in \mathbb{Z}$.

U sledećoj lemi navodimo osnovne osobine ove relacije. Svi dokazi su pravolinijski i ostavljamo ih za vežbu.

2. **Lema.** *(i) za sve $n \in \mathbb{Z}$ važi $n \mid n$ – refleksivnost;*
(ii) ako $k \mid m$ i $m \mid n$, onda $k \mid n$ – tranzitivnost;
(iii) za sve $n \in \mathbb{Z}$ važi $1 \mid n$ i $-1 \mid n$;
(iv) za sve $n \in \mathbb{Z}$ važi $n \mid 0$;
(v) ako $n \mid 1$ ili $n \mid -1$, onda $n = 1$ ili $n = -1$;
(vi) ako $0 \mid n$, onda $n = 0$;
(vii) ako $k \mid m$ i $k \mid n$, onda $k \mid am + bn$ za sve $a, b \in \mathbb{Z}$;
(viii) ako $m \mid n$, onda $am \mid an$ za sve $a \in \mathbb{Z}$;
(ix) ako $am \mid an$ i $a \neq 0$, onda $m \mid n$;
(x) ako $m \mid n$ i $n \neq 0$, onda $|m| \leqslant |n|$.

Datum trenutne verzije: 1. januar 2024.

II. **Lema o ostatku.**

3. **Lema** (Lema o ostatku). *Neka su* $a, b \in \mathbb{Z}$, $b > 0$. *Tada postoje jedinstveni* $q, r \in \mathbb{Z}$ *takvi da* $a = qb + r$ *i* $0 \leqslant r < b$.

Jedinstveni broj q *je* količnik *pri celobrojnom deljenju* a *sa* b, *a jedinstveni broj* r *je* ostatak *pri celobrojnom deljenju* a *sa* b.

Dokaz. Dokažimo najpre jedinstvenost brojeva q i r. Pretpostavimo da možemo da zapišemo $a = bq_1 + r_1$ i $a = bq_2 + r_2$, gde $0 \leqslant r_1, r_2 < b$. Primetimo da je tada $0 \leqslant |r_1 - r_2| < b$. Oduzimanjem dve jednakosti dobijamo $b(q_1 - q_2) + (r_1 - r_2) = 0$, tj. $b(q_1 - q_2) = r_2 - r_1$. Tada $b \mid r_2 - r_1$, pa i $b \mid |r_1 - r_2|$, odakle $|r_1 - r_2| = 0$ ili $b < |r_1 - r_2|$. Kako smo već uočili $|r_1 - r_2| < b$, zaključujemo $|r_1 - r_2| = 0$, odakle $r_1 = r_2$. Vraćanjem u jednakost $b(q_1 - q_2) = r_2 - r_1 = 0$ dobijamo i $q_1 - q_2 = 0$ jer $b > 0$, odnosno $q_1 = q_2$. Time smo dokazali željenu jedinstvenost.

Sada ćemo da dokažemo egzistenciju brojeva q i r. U prvom koraku pretpostavićemo da je $a \leqslant 0$. Dokaz izvodimo potpunom indukcijom po a. Neka je $a \geqslant 0$ proizvoljan broj. Posmatrajmo broj $a - b$ i primetimo $a - b < a$. Imamo dva slučaja:

1° Ako $a - b \geqslant 0$, po indukcijskoj hipotezi postoje brojevi q i r takvi da $a - b = qb + r$ i $0 \leqslant r < b$. Tada je $a = (q+1)b + r$ i $0 \leqslant r < b$, pa smo našli željeni količnik $q + 1$ i ostatak r.

2° Ako $a - b < 0$, onda je $a < b$, pa možemo da zapišemo $a + 0 \cdot b + a$ i $0 \leqslant a < b$, i ponovo smo našli odgovarajući količnik 0 i ostatak a.

Time smo dokazali egzistenciju za $a \geqslant 0$. Pretpostavimo sada da je $a < 0$. Prema prethodnom delu dokaza, postoje q i r takvi da $-a = qb + r$ i $0 \leqslant r < b$. Imamo dva slučaja:

1° Ako $r = 0$, tj. $-a = qb$, imamo $a = (-q)b$ i našli smo odgovarajući količnik $-q$ i ostatak 0.

2° Ako $0 < r < b$, tada je $0 < b - r < b$ i $a = (-q)b - r = (-q - 1)b + (b - r)$, i ponovo smo našli odgovarajući količnik $-q - 1$ i ostatak $b - r$. Ω

4. *Komentar.* Lema o ostatku ima i jaču varijantu. Za $a, b \in \mathbb{Z}$, $b \neq 0$, postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da $a = qb + r$ i $0 \leqslant r < |b|$.

Za $b > 0$ u pitanju je baš lema o ostatku. Ako je $b < 0$, po lemi o ostatku postoje $q, r \in \mathbb{Z}$ takvi da $a = q(-b) + r$ i $0 \leqslant r < -b = |b|$. Tada je naravno i $a = (-q)b + r$, pa je odgovarajući količnik $-q$ i ostatak r.

Jedinstvenost dokazujemo na identičan način kao i u dokazu leme o ostatku.

III. **NZD, Euklidov algoritam i Bezuova lema.**

5. **Definicija.** Broj $d \geqslant 0$ je *najveći zajednički delilac* (*NZD*) brojeva $a, b \in \mathbb{Z}$, pišemo $(a, b) = d$, ako:

- $d \mid a$ i $d \mid b$, tj. d jeste zajednički delilac od a i b;
- ako $e \mid a$ i $e \mid b$, onda i $e \mid d$, tj. d je najveći zajednički delilac.

Broj $s \geqslant 0$ je *najmanji zajednički sadržalac* (*NZS*) brojeva $a, b \in \mathbb{Z}$, pišemo $[a, b] = s$, ako:

- $a \mid s$ i $b \mid s$, tj. s jeste zajednički sadržalac od a i b;
- ako $a \mid t$ i $b \mid t$, onda i $s \mid t$, tj. s je najmanji zajednički sadržalac.

6. **Primer.** Neka $a, b \in \mathbb{Z}$, $a \geqslant 0$. Lako vidimo sledeće činjenice:

- $(a, b) = a$ akko $a \mid b$, i $[a, b] = a$ akko $b \mid a$;
- specijalno, $(a, 0) = a$ i $[a, 0] = 0$, i $(a, 1) = 1$ i $[a, 1] = a$;
- $(a, b) = (-a, b) = (a, -b) = (-a, -b)$ i $[a, b] = [-a, b] = [a, -b] = [-a, -b]$.

Prethodna tvrđenja direktno se dokazuju.

Prema prethodnom primeru (poslednja tačka) možemo da se fokusiramo na prirodne a i b.

7. **Lema.** *Ako je* $a = bq + c$, *onda je* $(a, b) = (b, c)$.

Dokaz. Označimo sa $D(x, y)$ skup zajedničkih delilaca brojeva x i y. Dovoljno je da primetimo da je $D(a, b) = D(b, c)$. Ako $d \in D(a, b)$, tada $d \mid a$ i $d \mid b$, pa $d \mid a - bq = c$; dakle, $d \mid b$ i $d \mid c$, tj. $d \in D(b, c)$. Obratno, ako $d \in D(b, c)$, tada $d \mid b$ i $d \mid c$, pa $d \mid bq + c = a$; dakle, $d \mid a$ i $d \mid b$, tj. $d \in D(a, b)$. Dokazali smo da je $D(a, b) = D(b, c)$. Ω

Sada ćemo opisati *Euklidov algoritam* za nalaženje NZD-a. Neka su $a, b > 0$ proizvoljni. Definišimo (ispostaviće se, konačan) niz prirodnih brojeva r_i na sledeći način:

- $r_0 := a$ i $r_1 := b$;
- pretpostavimo da smo definisali niz do r_i, $i \geqslant 1$. Ako je $r_i = 0$ završili smo postupak. Ako $r_i > 0$, po lemi o ostatku definišimo r_{i+1} da bude ostatak pri deljenju r_{i-1} sa r_i.

8. **Teorema.** *(i) Euklidov algoritam se završava, tj. za neko* n *biće* $r_n = 0$.
(ii) Ako je $r_n = 0$, *onda je* $(a, b) = r_{n-1}$.
(iii) (Bezuova lema) Postoje $p, q \in \mathbb{Z}$ *takvi da* $pa + qb = (a, b)$.

Dokaz. (i) Ako pretpostavimo da nijedan r_n nije nula (tj. da se algoritam ne završava u konačno mnogo koraka), po drugom koraku algoritma za sve $i \geqslant 1$ važi $r_{i+1} < r_i$, pa imamo beskonačan strogo opadajući niz prirodnih brojeva:

$$b = r_1 > r_2 > r_3 > \dots,$$

što nije moguće. Dakle, za neko n biće $r_n = 0$ i algoritam se završava.

(ii) Pretpostavimo da je $r_n = 0$. Tvrdimo da je $(a, b) = (r_{i-1}, r_i)$ za sve i, $1 \leqslant i \leqslant n$. Za $i = 1$ tvrđenje je očigledno. Nastavimo indukcijom. Pretpostavimo da je $(a, b) = (r_{i-1}, r_i)$. Po definiciji r_{i+1} imamo da je $r_{i-1} = r_i q + r_{i+1}$, pa je prema lemi 7, $(r_{i-1}, r_i) = (r_i, r_{i+1})$, odakle je $(a, b) = (r_i, r_{i+1})$. Time smo dokazali indukcijski korak.

Dakle, specijalno, $(a, b) = (r_{n-1}, r_n) = (r_{n-1}, 0) = r_{n-1}$.

(iii) Pretpostavimo da je $r_n = 0$. Tvrdimo da za sve $i = 1, \dots, n$, $(a, b) = pr_{i-1} + qr_i$ za neke cele p, q; specijalno, za $i = 1$ dobijamo $(a, b) = pr_0 + qr_1 = pa + qb$ za neke cele p, q, kao što želimo. Za $i = n$ imamo $(a, b) = r_{n-1} = 1 \cdot r_{n-1} + 0 \cdot r_n$, gde prva jednakost važi prema (ii). Nastavimo indukcijom (unazad, tj. korak oblika $i \mapsto i - 1$). Pretpostavimo da

$(a,b) = pr_{i-1}+qr_i$ za neke $p,q \in \mathbb{Z}$. Prema definiciji broja r_i imamo da je $r_{i-2} = r_{i-1}c+r_i$, tj. $r_i = r_{i-2} - r_{i-1}c$. Iz IH sada imamo $(a,b) = pr_{i-1} + qr_i = pr_{i-1} + q(r_{i-2} - r_{i-1}c) = qr_{i-2} + (p-qc)r_{i-1} = p'r_{i-2} + q'r_{i-1}$ za $p' = q$ i $q' = p - qc$. Time smo dokazali indukcijski korak. Ω

Sada ćemo opisati još jedan postupak za nalaženje NZD-a kao i jedan par koeficijenata p,q datih u Bezuovoj lemi. Neka su a,b proizvoljni brojevi za koje želimo da izračunamo (a,b), kao i neke brojeve p,q takve da $(a,b) = pa + qb$. Počinjemo sa 2×3 matricom:

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Sada izvodimo niz matrica tako što u svakom koraku vršimo sledeću transformaciju: jednoj od vrsta matrice dodajemo drugu umnoženu nekim celim brojem. Npr. dodavanje umnožene prve vrste matrice sa $\lambda \in \mathbb{Z}$ drugoj vrsti izgleda ovako:

$$\begin{bmatrix} x & \alpha & \beta \\ y & \gamma & \delta \end{bmatrix} \begin{matrix} \\ \downarrow \cdot\lambda \end{matrix} \rightsquigarrow \begin{bmatrix} x & \alpha & \beta \\ y+\lambda x & \gamma+\lambda\alpha & \delta+\lambda\beta \end{bmatrix}$$

Postupak nastavljamo dok ne dobijemo matricu koja ima 0 u prvoj koloni, npr. u prvoj vrsti:

$$\begin{bmatrix} 0 & - & - \\ d & p & q \end{bmatrix}$$

Brojevi d,p,q u drugoj vrsti su takvi da $d = pa + qb$. Takođe, ako $d > 0$, $(a,b) = d$ pa je i $(a,b) = pa + qb$, a ako je $d < 0$, onda je $(a,b) = -d$ pa je i $(a,b) = (-p)a + (-q)b$.

Primetimo da do nule u prvoj koloni uvek možemo da dođemo. Naime, ako su u prvoj koloni brojevi x i y, npr. pozitivni (ako je neki negativan slično ćemo postupiti), takvi da je $x > y$, dovoljno je da zapišemo $x = yq + r$ gde $0 \leqslant r < y$ i da vrstu kojoj je y pomnožimo sa $-q$ i dodamo vrsti u kojoj je x. Ovaj postupak strogo smanjuje maksimum brojeva prve kolone, pa nastavljajući ovakav postupak u konačno mnogo koraka moramo doći do nule. Inače, nije obavezno da ovako postupimo. Možda u konkretnim slučajevima možemo da postupimo na drugačiji način i brže dođemo do rešenja, ili da postupamo postepenije jer je izračunavanje brojeva q i r nepraktično (ako su veliki brojevi u pitanju).

Pre nego što objasnimo prethodni postupak, uradimo jedan primer.

9. **Primer.** Nađimo $(483, 637)$ i brojeve p i q takve da je $(161, 637) = 161p + 637q$.

$$\begin{bmatrix} 483 & 1 & 0 \\ 637 & 0 & 1 \end{bmatrix} \begin{matrix} \\ \downarrow \cdot(-1) \end{matrix} \quad \begin{bmatrix} 483 & 1 & 0 \\ 154 & -1 & 1 \end{bmatrix} \begin{matrix} \\ \downarrow \cdot(-3) \end{matrix} \quad \begin{bmatrix} 21 & 4 & -3 \\ 154 & -1 & 1 \end{bmatrix} \begin{matrix} \\ \downarrow \cdot(-7) \end{matrix}$$

$$\begin{bmatrix} 21 & 4 & -3 \\ 7 & -29 & 22 \end{bmatrix} \begin{matrix} \\ \downarrow \cdot(-3) \end{matrix} \quad \begin{bmatrix} 0 & * & * \\ 7 & -29 & 22 \end{bmatrix}$$

(Primetimo da $*$ ne moramo da izračunamo jer smo već našli 0.) Dakle, $(483, 637) = 7$ i $7 = -29 \cdot 483 + 22 \cdot 637$.

Objasnimo sada korektnost postupka. Uočimo jedan korak:

$$\begin{bmatrix} x & \alpha & \beta \\ y & \gamma & \delta \end{bmatrix} \begin{matrix} \\ \cdot\lambda \end{matrix} \rightsquigarrow \quad \begin{bmatrix} x & \alpha & \beta \\ y+\lambda x & \gamma+\lambda\alpha & \delta+\lambda\beta \end{bmatrix}$$

Najpre, prema lemi 7, $(x, y+\lambda x) = (x, y)$ pa naša transformacija čuva NZD elemenata u prvoj koloni. Kako prvu kolonu polazne matrice čine elementi a i b, i u svakom koraku se čuva NZD elemenata prve kolone, (a, b) jednak je NZD-u elemenata u prvoj koloni krajnje matrice, tj. $(a, b) = (0, d)$ što je jednako d ako je $d > 0$ i $-d$ ako je $d < 0$. Takođe, ako pretpostavimo da važe jednakosti $x = \alpha a + \beta b$ i $y = \gamma a + \delta b$ (pročitane iz leve matrice), tada i odgovarajuće jednakosti važe i za desnu matricu. Jednakost $x = \alpha a + \beta b$ ostaje, a jednakost $y + \lambda x = (\gamma + \lambda\alpha)a + (\delta + \lambda\beta)b$ važi jer:

$$y + \lambda x = (\gamma a + \delta b) + \lambda(\alpha a + \beta b) = (\gamma + \lambda\alpha)a + (\delta + \lambda\beta)b.$$

S obzirom da polazna matrica zadovoljava ove jednakosti: $a = 1 \cdot a + 0 \cdot b$ i $b = 0 \cdot a + 1 \cdot b$, i transformacija čuva ovu osobinu, i krajnja matrica u postupku zadovoljava ovu osobinu, tj. važi $d = pa + qb$, kao što i tvrdimo.

IV. **Uzajamno prosti brojevi.**

10. **Definicija.** Brojevi $a, b \in \mathbb{Z}$ su *uzajamno prosti* ako $(a, b) = 1$.

11. **Tvrđenje.** *Neka $a, b \in \mathbb{Z}$. Tada $(a, b) = 1$ akko postoje $p, q \in \mathbb{Z}$ takvi da $pa + qb = 1$.*

Dokaz. Smer ($\Rightarrow$) sledi prema Bezuovoj lemi. Smer ($\Leftarrow$) je očigledan jer kako $(a, b) \mid a$ i $(a, b) \mid b$, tada $(a, b) \mid pa + qb$, tj. $(a, b) \mid 1$, odakle $(a, b) = 1$ (jer je NZD po definiciji nenegativan). Ω

12. **Tvrđenje.** *(i) Ako $(m_1, n) = (m_2, n) = 1$, onda i $(m_1 m_2, n) = 1$;*
(ii) ako $(m_1, n) = (m_2, n) = \cdots = (m_k, n) = 1$, onda i $(m_1 m_2 \ldots m_k, n) = 1$;
(iii) ako $(m_1, m_2) = 1$, $m_1 \mid s$ i $m_2 \mid s$, onda i $m_1 m_2 \mid s$;
(iv) ako su $m_1, m_2, \ldots, m_k$ međusobno uzajamno prosti, $m_i \mid s$ za sve i, $1 \leqslant i \leqslant k$, onda i $m_1 m_2 \ldots m_k \mid s$.

Dokaz. (i) Neka su $(m_1, n) = (m_2, n) = 1$. Prema prethodnom tvrđenju zapišimo $pm_1 + qn = 1$ i $p'm_2 + q'n = 1$. Ako pomnožimo ove dve jednakosti dobijamo $(pp')m_1 m_2 + (pq'm_1 + p'qm_2 + qq'n)n = 1$, pa prema prethodnom tvrđenju važi $(m_1 m_2, n) = 1$.

(ii) Indukcijom po k koristeći (i).

(iii) Iz $(m_1, m_2) = 1$ zapišimo $pm_1 + qm_2 = 1$, a iz $m_1 \mid s$ zapišimo $s = m_1 c$. Množenjem prve jednakosti sa c dobijamo $ps + qm_2 c = c$, pa kako $m_2 \mid s$, m_2 deli levu stranu jednakosti pa i $m_2 \mid c$. Ako zapišemo $c = m_2 d$, vraćajući se imamo $s = m_1 c = m_1 m_2 d$, tj. $m_1 m_2 \mid s$.

(iv) Indukcijom po k koristeći (ii) i (iii). Ω

13. **Lema.** *Ako je bar jedan od $a, b \in \mathbb{Z}$ nenula i $d = (a, b)$, onda su $\frac{a}{d}$ i $\frac{b}{d}$ uzajamno prosti.*

Dokaz. Pretpostavimo da je $e > 0$ takav da $e \mid \frac{a}{d}$ i $e \mid \frac{b}{d}$. Tada očigledno $de \mid a$ i $de \mid b$, pa $de \mid d$ jer je $d = (a, b)$, odakle sledi $e = 1$. Dakle, jedini pozitivni zajednički delilac brojeva $\frac{a}{d}$ i $\frac{b}{d}$ je 1, pa je $(\frac{a}{d}, \frac{b}{d}) = 1$. Ω

14. **Tvrđenje.** *Ako* $c \mid ab$ *i* $(c,a)=1$, *onda* $c \mid b$.

Dokaz. Po Bezuovoj lemi neka su $p,q \in \mathbb{Z}$ takvi da $pc+qa=1$. Množenjem sa b dobijamo $pcb+qab=b$. Primetimo da c deli levu stranu jer očigledno deli prvi sabirak, a deli i drugi sabirak jer deli ab. Prema tome, c deli i desnu stranu, tj. $c \mid b$. Ω

15. **Lema.** *Pretpostavimo* $a,b>0$. *Tada je* $ab=(a,b)[a,b]$.

Dokaz. Označimo $s=\frac{ab}{(a,b)}$. Kako je $s=a\frac{b}{(a,b)}=\frac{a}{(a,b)}b$, s je ceo broj, $a \mid s$ i $b \mid s$. Pretpostavimo $a \mid t$ i $b \mid t$, treba samo da dokažemo $s \mid t$. Zapišimo $t=aa'$ i $t=bb'$. Tada je $aa'=bb'$, odakle je i $\frac{a}{(a,b)}a'=\frac{b}{(a,b)}b'$. Odavde sledi $\frac{a}{(a,b)} \mid \frac{b}{(a,b)}b'$, pa kako i $(\frac{a}{(a,b)},\frac{b}{(a,b)})=1$ po lemi 13, dobijamo $\frac{a}{(a,b)} \mid b'$ po tvrđenju 14. Dakle, $b'=\frac{a}{(a,b)}k$ za neko k, pa je $t=bb'=\frac{ab}{(a,b)}k=sk$, odakle $s \mid t$. Završili smo dokaz. Ω

U opštem slučaju, ako $a,b \in \mathbb{Z}$, ab je do na znak jednako $(a,b)[a,b]$.

V. **Linearna diofantovska jednačina sa dve nepoznate.** Linearna diofantovska jednačina sa dve nepoznate je jednačina oblika $aX+bY=c$ gde su koeficijenti $a,b,c \in \mathbb{Z}$, $a,b \neq 0$, i čija rešenja tražimo u skupu $\mathbb{Z}$.

16. **Teorema.** *Jednačina* $aX+bY=c$ *ima rešenje akko* $(a,b) \mid c$. *Ako je* (x_0,y_0) *jedno rešenje, onda su sva rešenja data po formuli:*

$$\begin{aligned} x &= x_0 - k\frac{b}{(a,b)} \\ y &= y_0 + k\frac{a}{(a,b)} \end{aligned}$$

gde je $k \in \mathbb{Z}$ *proizvoljno.*

Dokaz. Najpre ćemo da razmotrimo problem egzistencije rešenja. Ako je (x_0,y_0) jedno rešenje jednačine, tj. $ax_0+by_0=c$, kako $(a,b) \mid a$ i $(a,b) \mid b$, onda $(a,b) \mid ax_0+by_0$, tj. $(a,b) \mid c$. Obratno, ako $(a,b) \mid c$, onda je $\frac{c}{(a,b)} \in \mathbb{Z}$. Po Bezuovoj lemi postoje $p,q \in \mathbb{Z}$ takvi da je $pa+bq=(a,b)$, pa množenjem ove jednakosti sa $\frac{c}{(a,b)}$ dobijamo $\frac{pc}{(a,b)}a+\frac{qc}{(a,b)}b=c$, tj. $x_0=\frac{pc}{(a,b)}$ i $y_0=\frac{qc}{(a,b)}$ je jedno rešenje naše jednačine.

Naglasimo da je u prethodnom dokazu opisano kako dolazimo do jednog rešenja.

Opišimo sada sva rešenja ako ona postoje, tj. ako $(a,b) \mid c$. Neka je (x_0,y_0) jedno fiksirano rešenje i neka je (x,y) proizvoljno rešenje. Dakle imamo:

$$\begin{aligned} ax+by &= c \\ ax_0+by_0 &= c \end{aligned}$$

Oduzimanjem ove dve jednakosti dobijamo $a(x-x_0)+b(y-y_0)=0$, tj. $a(x-x_0)=-b(y-y_0)$. Deljenjem sa (a,b) dobijamo:

$$\frac{a}{(a,b)}(x-x_0)=-\frac{b}{(a,b)}(y-y_0).$$

Prema lemi 13, $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$, pa kako $\frac{a}{(a,b)} \mid \frac{a}{(a,b)}(x-x_0)$ to $\frac{a}{(a,b)} \mid -\frac{b}{(a,b)}(y-y_0)$, odakle prema tvrđenju 14 sledi $\frac{a}{(a,b)} \mid y-y_0$, tj. $y = y_0 + k\frac{a}{(a,b)}$ za neko $k \in \mathbb{Z}$. Vraćanjem u gornju jednakost dobijamo:

$$\frac{a}{(a,b)}(x-x_0) = -\frac{b}{(a,b)}k\frac{a}{(a,b)},$$

pa deljenjem sa $\frac{a}{(a,b)}$ dobijamo:

$$(x-x_0) = -k\frac{b}{(a,b)},$$

odakle je $x = x_0 - k\frac{b}{(a,b)}$, kao što smo i želeli.

Sa druge strane, nije teško proveriti da su svi parovi dati sa $x = x_0 - k\frac{b}{(a,b)}$ i $y = y_0 + k\frac{a}{(a,b)}$ gde $k \in \mathbb{Z}$ rešenja jednačine. Ω

17. **Primer.** Rešiti jednačine $198X - 93Y = 5$ i $198X - 93Y = 6$.

Najpre ćemo da nađemo $(198, 93)$ i brojeve p, q takve da $198p + 93q = (198, 93)$:

$$\begin{bmatrix} 198 & 1 & 0 \\ 93 & 0 & 1 \end{bmatrix} \overset{\cdot(-2)}{\leftarrow} \quad \begin{bmatrix} 12 & 1 & -2 \\ 93 & 0 & 1 \end{bmatrix} \overset{\cdot(-8)}{\leftarrow} \quad \begin{bmatrix} 12 & 1 & -2 \\ -3 & -8 & 17 \end{bmatrix} \overset{\cdot 4}{\leftarrow} \quad \begin{bmatrix} 0 & * & * \\ -3 & -8 & 17 \end{bmatrix}$$

Dakle, $(198, 93) = 3$ i $3 = 8 \cdot 198 - 17 \cdot 93$. Kako $3 \nmid 5$, prva jednačina nema rešenja. Množenjem prethodne jednakosti sa 2 dobijamo $16 \cdot 198 - 34 \cdot 93 = 6$, tj. $x_0 = 16$ i $y_0 = 34$ je jedno rešenje druge jednačine. Sada sva rešenja dobijamo po formuli:

$$\begin{aligned} x &= 16 - k\frac{-93}{3} = 16 + 31k \\ y &= 34 + k\frac{198}{3} = 34 + 66k \end{aligned}$$

gde $k \in \mathbb{Z}$.

VI. Prosti brojevi.

18. **Definicija.** Broj $p > 1$ je *prost* ako su mu jedini pozitivni delioci 1 i p.

19. **Teorema.** *Broj $p > 1$ je prost akko $(\forall a, b \in \mathbb{Z})(p \mid ab \to p \mid a \vee p \mid b)$.*

Dokaz. ($\Rightarrow$) Neka je $p > 1$ prost broj, i neka $p \mid ab$. Pretpostavimo $p \nmid a$ i dokažimo $p \mid b$. Tvrdimo $(p, a) = 1$. Zaista, ako je $(p, a) = d$, onda $d \mid p$ pa je $d = 1$ ili $d = p$. Kako $d = p$ znači i da $p = d \mid a$ dobijamo $p \mid a$, što smo pretpostavili da nije. Dakle, $d = 1$, tj. $(p, a) = 1$. Iz $p \mid ab$ i $(p, a) = 1$ sada zaista sledi $p \mid b$ po lemi 14.

($\Leftarrow$) Pretpostavimo da $p > 1$ nije prost. To znači da ima delilac a takav da $1 < a < p$. Označimo $b = \frac{p}{a}$; očigledno i $1 < b < p$. Pa imamo $p \mid p = ab$ ali $p \nmid a$ i $p \nmid b$. Ω

20. **Teorema.** *Svaki broj $n > 1$ je ili prost ili jednak proizvodu prostih brojeva.*

Dokaz. Dokaz izvodimo potpunom indukcijom po $n > 1$. Neka je $n > 1$. Ako je n prost nemamo šta da pokažemo. Ako n nije prost on ima delilac a takav da $1 < a < n$. Ako je $b = \frac{n}{a}$ tada je očigledno i $1 < b < n$. Prema tome i za a i za b možemo da primenimo

indukcijsku hipotezu, tj. svaki od njih je ili prost ili je jednak proizvodu prostih. Očigledno, $n = ab$ je jednak proizvodu prostih. Ω

Kao direktnu posledicu prethodne teoreme imamo:

21. **Tvrđenje.** *Svaki broj $n > 1$ deljiv je nekim prostim brojem.*

22. **Teorema** (Euklid)**.** *Postoji beskonačno mnogo prostih brojeva.*

Dokaz. Pretpostavimo suprotno, neka su $p_1, p_2, \ldots, p_k$ svi prosti brojevi. Uočimo broj $n = p_1 p_2 \ldots p_k + 1$. Broj n očigledno nije deljiv ni jednim od brojeva $p_1, \ldots, p_k$ (n daje ostatak 1 pri deljenju sa svakim od p_i), a kako smo pretpostavili da su to svi prosti brojevi, n nije deljiv ni sa jednim prostim brojem. Ovo je u suprotnosti sa prethodnim tvrđenjem. Ω

23. **Teorema** (Osnovna teorema aritmetike)**.** *Svaki broj $n > 1$ zapisuje se, do na raspored činioca, na jedinstven način kao proizvod prostih brojeva.*[1]

Dokaz. Već smo videli da se svaki broj $n > 1$ može zapisati kao proizvod prostih brojeva. Označimo sa $\alpha(n)$ najmanji broj prostih brojeva potrebnih da bi se n zapisao kao njihov proizvod (npr. $\alpha(2) = 1$ jer je 2 prost broj, $\alpha(12) = 3$ jer je $12 = 2 \cdot 2 \cdot 3$, $\alpha(15) = 2$ jer je $15 = 3 \cdot 5$, itd.).

Potpunom indukcijom po $\alpha(n)$ dokazaćemo da je zapis u proizvod prostih, do na raspored činilaca, jedinstven. Neka je $k \geqslant 1$ proizvoljan i neka je $\alpha(n) = k$. Razmotrićemo dva slučaja.

Ako je $k = 1$, tada je n prost i znamo da ga ne možemo zapisati kao proizvod drugih prostih (jer n nema delioce različite od 1 i n).

Neka je $k > 1$. Zapišimo $n = p_1 p_2 \ldots p_k$, gde su p_i prosti, i pretpostavimo $n = q_1 q_2 \ldots q_l$, gde je $l \geqslant k$ i q_j su takođe prosti. Dokazaćemo da je $l = k$ i da su ova dva zapisa, do na raspored činilaca, jednaki. Kako je:

$$p_1 \ldots p_k = q_1 \ldots q_l,$$

imamo $p_k \mid q_1 q_2 \ldots q_l$. Kako je p_k prost prema teoremi 19, $p_k \mid q_j$ za neko j, $1 \leqslant j \leqslant l$. Kako je i q_j prost, $p_k = q_j$, pa deljenjem gornje jednakosti sa p_k dobijamo:

$$p_1 \ldots p_{k-1} = q_1 \ldots q_{j-1} q_{j+1} \ldots q_l.$$

Označimo ovaj broj sa m i primetimo $m > 1$ jer $k > 1$. Primetimo da je $\alpha(m) \leqslant k - 1 < k$ (zapravo možemo da diskutujemo da je $\alpha(m) = k - 1$, ali to nam za dokaz nije bitno). Po indukcijskoj hipotezi, do na raspored činilaca, m se na jedinstven način može zapisati kao proizvod prostih. To znači da su brojevi $q_1, \ldots, q_{j-1}, q_{j+1}, \ldots, q_l$ samo ispermutovani brojevi $p_1, \ldots, p_{k-1}$. Dakle, i brojevi $q_1, \ldots, q_l$ su samo ispermutovani brojevi $p_1, \ldots, p_k$ (vraćanjem $p_k = q_j$ u niz). Time smo završili dokaz. Ω

[1] Podrazumevamo da je prost broj p jednak proizvodu u kome učestvuje samo jedan činilac.

VII. **Kongruencija modulo** m**.** Već smo videli da za $m \geqslant 2$ na $\mathbb{Z}$ imamo ekvivalenciju $\equiv_m$ definisanu sa $a \equiv_m b$ akko $m \mid a - b$. Dokazaćemo da ova relacija zadovoljava i dodatne osobine.

24. **Tvrđenje.** *Neka* $a \equiv_m a'$ *i* $b \equiv_m b'$*. Tada:*

(i) $a + b \equiv_m a' + b'$*;*
(ii) $ab \equiv_m a'b'$*;*
(iii) $a^n \equiv_m a'^n$ *za sve* $n \geqslant 1$*.*

Dokaz. (i) Ovo sledi jer $(a + b) - (a' + b') = (a - a') + (b - b')$ i m deli oba sabirka na desnoj strani.

(ii) Imamo $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b')$ i m deli oba sabirka na desnoj strani.

(iii) Indukcijom po n koristeći (ii). Ω

Takođe, ako $a+b \equiv_m a'+b'$ i $b \equiv_m b'$, možemo da skratimo b i b', i da dobijemo $a \equiv_m a'$. (Zaista, možemo da zapišemo $a - a' = ((a + b) - (a' + b')) - (b - b')$, i oba sabirka su deljiva sa m.) Međutim, u opštem slučaju, skraćivanje kod množenja nije dozvoljeno, tj. $ab \equiv_m a'b'$ i $b \equiv_m b'$ u opštem slučaju ne povlače $a \equiv_m a'$. Npr. $2 \cdot 6 \equiv_4 3 \cdot 6$ i $6 \equiv_4 6$, ali nije $2 \equiv_4 3$.

Međutim, ako je ispunjen dodatni uslov, možemo da skratimo.

25. **Tvrđenje.** *Ako* $ab \equiv_m a'b'$*,* $b \equiv_m b'$ *i* $(b, m) = 1$*, onda* $a \equiv_m a'$*.*

Dokaz. Najpre primetimo da $b \equiv_m b'$ znači da možemo zapisati $b' = b + rm$, pa je $ab \equiv_m a'b' = a'(b+rm) = a'b+a'rm \equiv_m a'b+0 = a'b$, odakle $m \mid ab-a'b = (a-a')b$. Iz $(b, m) = 1$, zapišimo $pb+qm = 1$. Množenjem sa $(a-a')$ dobijamo $a-a' = pb(a-a')+qm(a-a')$. Kako m deli oba sabirka na desnoj strani, deli i $a - a'$, tj. $a \equiv_m a'$. Ω

26. **Definicija.** Broj b je *inverz od* a *modulo* m ako $ab \equiv_m 1$.

27. **Tvrđenje.** *Inverz od* a *modulo* m *postoji akko* $(a, m) = 1$*. U tom slučaju, ako je* b *jedan inverz, svi ostali inverzi su opisani formulom* $x = b + km$*,* $k \in \mathbb{Z}$*, što znači da* a *ima jedinstven inverz* x *takav da* $1 \leqslant x < m$*.*

Dokaz. Ako je $ab \equiv_m= 1$, tada $ab - 1 = km$ ili $ab - km = 1$ odakle $(a, m) = 1$. Sa druge strane, ako $(a, m) = 1$, zapišimo $pa + qm = 1$. Očigledno je $pa \equiv_m 1$, tj. a ima inverz modulo m.

Neka je b jedan fiksirani inverz i x proizvoljan inverz. Tada $ab \equiv_m 1 \equiv_m ax$, pa kako $(a, m) = 1$ skraćivanje sa a dobijamo $b \equiv_m x$, pa je $x = b + km$ za neko $k \in \mathbb{Z}$. Obratno, ako je $x = b + km$, onda je $ax = ab + akm \equiv_m ab \equiv_m 1$, tj. x je inverz od a modulo b. Ω

VIII. **Kineska teorema o ostacima.**

28. **Teorema** (Kineska teorema o ostacima). *Neka su $m_1, m_2, \dots, m_k \geqslant 2$ međusobno uzajamno prosti brojevi i $a_1, a_2, \dots, a_k \in \mathbb{Z}$. Sistem kongruencija:*

$$\begin{aligned} x &\equiv_{m_1} a_1 \\ x &\equiv_{m_2} a_2 \\ &\vdots \\ x &\equiv_{m_k} a_k \end{aligned}$$

ima rešenje. Ako je x_0 jedno rešenje, tada sva rešenja su data formulom:

$$x = x_0 + nM,\ n \in \mathbb{Z},$$

gde je $M = m_1 m_2 \dots m_k$. Specijalno, postoji jedinstveno rešenje x_0 tako da $0 \leqslant x_0 < M$, koje zovemo osnovno rešenje sistema.

Dokaz. Za početak ćemo pretpostaviti da imamo rešenje x_0 gornjeg sistema, i dokazaćemo drugi deo tvrđenja. Neka je x neko rešenje sistema. Kako za sve i, $1 \leqslant i \leqslant k$, važi $x_0 \equiv_{m_i} a_i$ i $x \equiv_{m_i} a_i$, imamo i $x_0 \equiv_{m_i} x$, tj. $m_i \mid x - x_0$. Po tvrđenju 12(iv), $M \mid x - x_0$, tj. postoji $n \in \mathbb{Z}$ tako da $x - x_0 = nM$, tj. $x = x_0 + nM$.

Sa druge strane, za proizvoljno $n \in \mathbb{Z}$ element $x = x_0 + nM$ jeste rešenje sistema jer $x_0 + nM \equiv_{m_i} x_0$ jer $m_i \mid M$. Dakle, sva rešenja jesu navedenog oblika.

Sada je jasno da postoji jedistveno rešenje x_0 takvo da $0 \leqslant x_0 < M$, i to je ostatak pri deljenju x sa M, gde je x bilo koje rešenje sistema (kako smo videli sva rešenja imaju isti ostatak pri deljenju sa M).

Dakle, ostaje da nađemo bar jedno rešenje. Označimo sa $M_i = \frac{M}{m_i}$ za sve $i = 1, \dots, k$. Po tvrđenju 12(ii), $(M_i, m_i) = 1$ za sve $i = 1, \dots, k$. Po Bezuovoj lemi postoje $p_i, q_i \in \mathbb{Z}$ tako da $p_i M_i + q_i m_i = 1$ za sve $i = 1, \dots, k$. Dokažimo da je:

$$x_0 = p_1 M_1 a_1 + p_2 M_2 a_2 + \dots + p_k M_k a_k$$

jedno rešenje sistema.

Neka je i, $1 \leqslant i \leqslant k$, proizvoljno. Tada $p_j M_j a_j \equiv_{m_i} 0$ za $j \neq i$ jer $m_i \mid M_j$. Dakle:

$$x_0 \equiv_{m_i} p_i M_i a_i.$$

(Svi ostali sabirci su nula.) Sa druge strane, $p_i M_i a_i \equiv_{m_i} a_i$ jer $p_i M_i + q_i m_i = 1$ povlači $p_i M_i \equiv_{m_i} 1$. Prema tome, $x_0 \equiv m_i a_i$. Dakle, x_0 zaista jeste jedno rešenje. Ω

Pored samog iskaza prethodne teoreme, bitno je da zapamtimo i algoritam konstrukcije proizvoljnog rešenja koji je dat u drugom delu dokaza. Ilustrujemo primenu jednim primerom.

29. **Primer.** Rešiti sistem kongruencija:

$$\begin{aligned} x &\equiv_3 2 \\ x &\equiv_4 1 \\ x &\equiv_{11} 7. \end{aligned}$$

Rešenje. Primetimo da je ispunjen uslov da su $3, 4, 11$ međusobo uzajamno prosti. Ispratićemo algoritam dat u dokazu kineske teoreme. Imamo $m_1 = 3$, $m_2 = 4$ i $m_3 = 11$, $a_1 = 2$, $a_2 = 1$ i $a_3 = 7$. Broj M je $M = m_1m_2m_3 = 3 \cdot 4 \cdot 11 = 132$; $M_1 = m_2m_3 = 44$, $M_2 = m_1m_3 = 33$, $M_3 = m_1m_2 = 12$. Najpre, treba da nađemo p_i i q_i tako da $p_iM_i + q_im_i = 1$ za sve $i = 1, 2, 3$.

Prvo, razmotrimo $M_1 = 44$ i $m_1 = 3$. Ovo nije teško da pogodimo: $(-1) \cdot 44 + 15 \cdot 3 = 1$, pa možemo da uzmemo $p_1 = -1$ i $q_1 = 15$. Za $M_2 = 33$ i $m_2 = 4$ isto je $1 \cdot 33 + (-8) \cdot 4 = 1$, pa uzmemo $p_2 = 1$ i $q_2 = -8$. Za $M_3 = 12$ i $m_3 = 11$, pa je $1 \cdot 12 + (-1) \cdot 11 = 1$, i uzmimo $p_3 = 1$ i $q_3 = -1$. Ako ne možemo da pogodimo rešenje iskoristili bismo Euklidov algoritam (ili neki drugi) da ga nađemo. Zapišimo sve sračunato u tabeli:

i	m_i	a_i	M_i	p_i	q_i
1	3	2	44	-1	15
2	4	1	33	1	-8
3	11	7	12	1	-1

Prema datom algoritmu jedno rešenje je $x_0 = p_1M_1a_1 + p_2M_2a_2 + p_3M_3a_3 = -88 + 33 + 84 = 29$. S obzirom da je $0 \leqslant 29 < 132$, $x_0 = 29$ je i osnovno rešenje sistema, dok su sva rešenja sistema data formulom $x = 29 + 132n$, $n \in \mathbb{Z}$. Ω

IX. **Ojlerova funkcija.**

30. **Definicija.** Za $n \geqslant 1$, sa U_n označavamo skup:

$$U_n = \{i \mid 1 \leqslant i \leqslant n,\ (i, n) = 1\},$$

dakle skup brojeva manjih od n koji su uzajamno prosti sa n. Broj elemenata skupa U_n obeležavamo sa $\varphi(n)$:

$$\varphi(n) := |U_n|,$$

dakle $\varphi(n)$ je broj elemenata koji su manji od n i uzajamno prosti sa n. Funkciju φ zovemo *Ojlerova funkcija*.

31. **Primer.** (1) Kako je $U_1 = \{1\}$, to je $\varphi(1) = 1$.
(2) Ako je p prost, $U_p = \{1, 2, 3, \ldots, p-1\}$, pa je $\varphi(p) = p - 1$.
(3) Ako je p prost, odredimo $\varphi(p^k)$. Broj $x \leqslant p^k$ uzajamno je prost sa p akko $p \nmid x$. Brojeva x takvi da $1 \leqslant x \leqslant p^k$ i $p \mid p^k$ ima p^{k-1}, to su: $p, 2p, 3p, \ldots, p^{k-1} \cdot p = p^k$. Prema tome, brojeva x za koje je $1 \leqslant x \leqslant p^k$ i $p \nmid x$, ima $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$.

Ispostavlja se da je račun iz prethodnog primera dovoljan da bismo u potpunosti odredili funkciju φ, tj. imamo sledeću teoremu:

32. **Teorema.** *Ako* $(m, n) = 1$, *onda je* $\varphi(mn) = \varphi(m)\varphi(n)$.

Dokaz. Dovoljno je da konstruišemo bijekciju $f : U_{mn} \to U_m \times U_n$. Definišemo:

$$f(k) = (k_m, k_n),$$

za $k \in U_{mn}$, gde sa k_m i k_n obeležavamo redom ostatke pri deljenju k sa m i n.

Primetimo da ako $k \in U_{mn}$, tj. $(k, mn) = 1$, tada je i $(k, m) = 1$ i $(k, n) = 1$, pa je i $(k_m, m) = 1$ i $(k_n, n) = 1$, odakle $k_m \in U_m$ i $k_n \in U_n$, što znači da je gornje preslikavanje zaista dobro deinisano.

f je 1-1: Neka $k, l \in U_{mn}$, bez umanjenja opštosti neka je $k \geqslant l$, i neka je $k_m = l_m$ i $k_n = l_n$; treba da dokažemo $k = l$. Kako je $k_m = l_m$, to znači $k \equiv_m l$, pa $m \mid k - l$, i slično $n \mid k - l$. Kako $(m, n) = 1$, to i $mn \mid k - l$, ali kako je $0 \leqslant k - l < mn$, to znači da $k - l = 0$, tj. $k = l$.

f je na: Neka su $a \in U_m$ i $b \in U_n$, tj. $(a, m) = 1$ i $(b, n) = 1$. Po kineskoj teoremi o ostacima imamo broj x takav da:

$$\begin{aligned} x &\equiv_m a \\ x &\equiv_n b \end{aligned}$$

i $0 \leqslant x < mn$. Kako je $x \equiv_m a$ i $(a, m) = 1$, to je $(x, m) = 1$, i slično $(x, n) = 1$, pa je i $(x, mn) = 1$. Dakle, $x \in U_{mn}$. Kako je očigledno $f(x) = (a, b)$, završili smo dokaz. Ω

33. **Posledica.** *Ako su $p_1, \ldots, p_s$ različiti prosti brojevi, tada je:*

$$\varphi(p_1^{k_1} \ldots p_s^{k_s}) = \varphi(p_1^{k_1}) \ldots \varphi(p_s^{k_s}) = (p_1^{k_1} - p_1^{k_1 - 1}) \ldots (p_s^{k_s} - p_s^{k_s - 1}),$$

odakle $\varphi(n) = n \prod_{p : p \mid n} (1 - \frac{1}{p})$.

X. **Ojlerova teorema.**

34. **Teorema** (Ojlerova teorema). *Neka su $n \geqslant 1$ i $a \in \mathbb{Z}$ takvi da $(n, a) = 1$. Tada:*

$$a^{\varphi(n)} \equiv_n 1.$$

Dokaz. Zapišimo $U_n = \{u_1, u_2, \ldots, u_{\varphi(n)}\}$. Neka su $r_1, r_2, \ldots, r_{\varphi(n)}$ redom ostaci pri deljenju $u_1 a, u_2 a, \ldots, u_{\varphi(n)} a$ sa n. Dokažimo:

$$\{r_1, r_2, \ldots, r_{\varphi(n)}\} = U_n.$$

Za svaki $i = 1, 2, \ldots \varphi(n)$ imamo $(u_i a, n) = 1$ jer $(u_i, n) = 1$ i $(a, n) = 1$, odakle i $(r_i, n) = 1$, pa $r_i \in U_n$. Dakle, važi inkluzija $(\subseteq)$. Kako levi skup ima najviše $\varphi(n)$ elemenata, a desni tačno $\varphi(n)$ elemenata, dovoljno je da dokažemo da za $i \neq j$ važi $r_i \neq r_j$. Neka $i \neq j$ i bez umanjenja opštosti pretpostavimo da je $u_i < u_j$. Tada $0 < u_j - u_i < n$, pa $n \nmid u_j - u_i$, a kako je i $(a, n) = 1$ imamo i $n \nmid (u_j - u_i)a$, pa $u_i a \not\equiv_n u_j a$, odakle $r_i \neq r_j$. Dokazali smo gornju jednakost. Sada je:

$$u_1 a \cdot u_2 a \cdots u_{\varphi(n)} a \equiv_n r_1 \cdot r_2 \cdots r_{\varphi(n)} = u_1 \cdot u_2 \cdots u_{\varphi(n)},$$

tj. $u \cdot a^{\varphi(n)} \equiv_n u$, gde je $u = u_1 \cdot u_2 \cdots u_{\varphi(n)}$. Dakle, $n \mid u(a^{\varphi(n)} - 1)$ pa $n \mid a^{\varphi(n)} - 1$ jer $(u, n) = 1$ jer je n uzajamno prost sa svim u_i. Dakle, $a^{\varphi(n)} \equiv_n 1$. Ω

35. **Posledica.** *Neka su $n \geqslant 1$ i $a \in \mathbb{Z}$ takvi da $(n, a) = 1$, i neka su $m, k \in \mathbb{N}$ takvi da $m \equiv_{\varphi(n)} k$. Tada $a^m \equiv_n a^k$.*

Dokaz. Dovoljno je da dokažemo $a^m \equiv_n a^r$ gde je r ostatak pri deljenju m sa $\varphi(n)$. Zapišimo $m = q\varphi(n) + r$. Tada je:

$$a^m = a^{q\varphi(n)+r} = (a^{\varphi(n)})^q a^r \equiv_n 1^q \cdot a^r = a^r,$$

gde je $a^{\varphi(n)} \equiv_n 1$ po Ojlerovoj teoremi. Ω

36. **Primer.** Izračunati ostatak pri deljenju $1234^{7865435}$ sa 11.

Rešenje. Kako je $1234 \equiv_{11} 2$, to je:

$$1234^{7865435} \equiv_{11} 2^{7865435}.$$

Kako je 11 prost, $11 \nmid 2$, $\varphi(11) = 11 - 1 = 10$ i $7865435 \equiv_{10} 5$, prema prethodnoj posledici je:

$$2^{7865435} \equiv_{11} 2^5 = 32 \equiv_{11} 10.$$

Dakle, traženi ostatak jednak je 10. Ω

37. **Primer.** Izračunati ostatak pri deljenju $28^{29^{30}}$ sa 13.

Rešenje. Kako je $28 \equiv_{13} 2$, to je:

$$28^{29^{30}} \equiv_{13} 2^{29^{30}}.$$

Kako je $(13, 2) = 1$ prema prethodnoj posledici potrebno je da izračunamo ostatak pri deljenju 29^{30} sa $\varphi(13) = 12$. Kako je $29 \equiv_{12} 5$, to je:

$$29^{30} \equiv_{12} 5^{30}.$$

Da bismo ovo pojednostavili možemo još jednom da idemo na Ojlerovu teoremu jer je $(12, 5) = 1$. Kako je $\varphi(12) = \varphi(3 \cdot 4) = 4$ i $30 \equiv_4 2$ imamo:

$$5^{30} \equiv_{12} 5^2 = 25 \equiv_{12} 1.$$

Vraćajući se unazad imamo:

$$2^{29^{30}} \equiv_{13} 2^1 = 2.$$

Dakle, traženi ostatak je 2. Ω

38. **Primer.** Odrediti dve poslednje cifre broja 3^{1234}.

Rešenje. Ako preformulišemo zadatak, treba da odredimo ostatak pri deljenju 3^{1234} sa 100. Jedan način je da primenimo Ojlerovu teoremu, koju možemo da primenimo jer $(3, 100) = 1$. Naime $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2)\varphi(5^2) = (2^2 - 2)(5^2 - 5) = 40$, i $1234 \equiv_{40} 34$, pa je prema prethodnoj posledici:

$$3^{1234} \equiv_{100} 3^{34}.$$

Sada možemo direktnim računom da dobijemo:

$$3^{34} = (3^5)^6 \cdot 3^4 = 243^6 \cdot 81 \equiv_{100} 43^6 \cdot 81 = (43^2)^3 \cdot 81 = 1849^3 \cdot 81 \equiv_{100} 49^3 \cdot 81 =$$
$$= 49^2 \cdot 49 \cdot 81 = 2401 \cdot 49 \cdot 81 \equiv_{100} 1 \cdot 49 \cdot 81 = 3969 \equiv_{100} 69.$$

Dakle, tražene poslednje dve cifre su 69.

Drugi način bi bio sledeći. Da izračunamo ostatke pri deljenju sa 4 i 25 pa da iskoristimo kinesku teoremu da nađemo ostatak pri deljenju sa 100. Za 4 je lako:

$$3^{1234} \equiv_4 (-1)^{1234} = 1.$$

Za 25, kako je $(3, 25) = 1$ možemo da iskoristimo Ojlerovu teoremu. Kako je $\varphi(25) = \varphi(5^2) = 5^2 - 5 = 20$ i $1234 \equiv_{20} 14$ imamo prema prethodnoj posledici:

$$3^{1234} \equiv_{25} 3^{14} = (3^3)^4 \cdot 3^2 = 27^4 \cdot 9 \equiv_{25} 2^4 \cdot 9 = 16 \cdot 9 = 144 \equiv_{25} = -6.$$

Sada tražimo osnovno rešenje sistema:

$$\begin{aligned} x &\equiv_4 1 \\ x &\equiv_{25} -6 \end{aligned}$$

Imamo $M = 100$, $m_1 = 4$, $M_1 = 25$, $m_2 = 25$ i $M_2 = 4$, pa kako je $(-6) \cdot 4 + 1 \cdot 25 = 1$, imamo tablicu:

i	m_i	a_i	M_i	p_i	q_i
1	4	1	25	1	-6
2	25	-6	4	-6	1

Jedno rešenje je $x = p_1 M_1 a_1 + p_2 M_2 a_2 = 25 + 144 = 169$, pa osnovno rešenje dobijamo uzimanjem ostatka pri deljenju sa 100, a to je 69. Ω

39. **Primer.** Odrediti dve poslednje cifre broja 2^{1234}.

Rešenje. Ponovo tražimo ostatak pri deljenju sa 100. Kako $(2, 100) \neq 1$, Ojlerovu teoremu ne možemo primeniti direktno. Ići ćemo na traženje ostatka pri deljenju sa 4 i 25 i kinesku teoremu. Za 4 je lako; očigledno $4 + 2^2 \mid 2^{1234}$, pa je $2^{1234} \equiv_4 0$. Za 25, kako $(2, 25) = 1$, možemo da idemo na Ojlerovu teoremu. Imamo $\varphi(25) = 20$ i $1234 \equiv_{20} = 14$, pa je prema prethodnoj posledici:

$$2^{1234} \equiv_{25} 2^{14} = (2^5)^2 \cdot 2^4 = 32^2 \cdot 16 \equiv_{25} 7^2 \cdot 16 = 49 \cdot 16 \equiv_{25} (-1) \cdot 16 = -16 \equiv_{25} 9.$$

Treba nam osnovno rešenje sistema:

$$\begin{aligned} x &\equiv_4 0 \\ x &\equiv_{25} 9 \end{aligned}$$

Imamo sličnu tablicu kao i u prethodnom primeru tablicu:

i	m_i	a_i	M_i	p_i	q_i
1	4	0	25	1	-6
2	25	9	4	-6	1

Jedno rešenje je $x = p_1 M_1 a_1 + p_2 M_2 a_2 = -216$, pa osnovno rešenje dobijamo uzimanjem ostatka pri deljenju sa 100, a to je 84. Dakle, tražene poslednje dve cifre su 84. Ω

XI. **RSA kriptosistem.** Opisaćemo jedna kriptosistem zasnovan na Ojlerovoj teoremi. Pretpostavimo da osoba B želi da pošalje osobi A tajnu poruku. Osoba B bi trebalo

nekako da šifruje poruku i pošalje je osobi A, ali tako da osoba A može da dešifruje poruku, ali i tako da treća strana C ne može da provali poruku.

Osoba A može da postupi na sledeći način. Najpre, izabere dva (u praksi velika) prosta broja p_A i q_A, izračuna $n_A = p_A q_A$ i $\varphi(n_A) = (p_A - 1)(q_A - 1)$. Zatim izabere broj s_A uzajamno prost sa $\varphi(n_A)$ i izračuna njegov inverz d_A modulo $\varphi(n_A)$.

Osoba A u ovom momentu može da zaboravi brojeve p_A, q_A i $\varphi(n_A)$. Osoba A objavljuje par (s_A, n_A) kao svoj (svima poznat) *javni ključ*, a čuva broj d_A kao svoj *tajni ključ*.

Osoba B pretvori (na neki već utvrđen način) željenu poruku u broj P takav da $P < n_A$, $(P, n_A) = 1$. Izračuna $P^{s_A} \equiv_{n_A} S$ tako da $S < n_A$ i šifrovanu poruku S šalje osobi A.

Osoba A tada računa $S^{d_A} \equiv_{n_A} D$ tako da $D < n_A$. Primetimo da je $D \equiv_{n_A} S^{d_A} \equiv_{n_A} P^{s_A d_A} \equiv_{n_A} P$ po Ojlerovoj teoremi jer je $(P, n_A) = 1$ i $s_A d_A \equiv_{\varphi(n_A)} = 1$. Kako je i $P, D < n_A$ zaključujemo $D = P$, tj. dešifrovana poruku D je baš originalna poruka P.

Da bi C provalio sistem, morao bi da izračuna d_A – inverz modulo $\varphi(n_A)$ od s_A. To može lako da uradi ako izaračuna $\varphi(n_A)$. Međutim, iako zna n_A, C ne može brzo (u razumnom vremenu) da nađe $\varphi(n_A)$ (brz algoritam za to nije poznat), pod uslovom da ne zna njegovu prostu faktorizaciju. Međutim, C ne može u razumnom vremenu ni da nađe prostu faktorizaciju broja n_A, jer ni za to brz algoritam nije poznat.

XII. **Vilsonova teorema.**

40. **Teorema** (Vilsonova teorema). *Neka $n \geqslant 2$. Broj n je prost akko $(n-1)! \equiv_n -1$.*

Dokaz. ($\Rightarrow$) Neka je n prost. Ako je $n = 2$, onda zaista važi $(2-1)! = 1! = 1 \equiv_2 -1$. Ako je $n = 3$, takođe imamo $(3-1)! = 2! = 2 \equiv_3 -1$. Pretpostavimo da je $n \geqslant 5$ neparan prost broj i zapišimo:

$$(n-1)! = 1 \cdot \underbrace{2 \cdots (n-2)}_{P} \cdot (n-1).$$

Dokazaćemo da činioce u proizvodu P, kojih ima $n-3$, možemo podeliti u $\frac{n-3}{2}$ parova tako da je proizvod svakog para modulo n jednak 1, što povlači i da je P modulo n jednako 1.

Dovoljno je da primetimo da za svako a, $2 \leqslant a \leqslant n-2$, postoji jedinstveno b tako da $2 \leqslant b \leqslant n-2$, $b \neq a$ i $ab \equiv_n 1$. Neka je a, $2 \leqslant a \leqslant n-2$ proizvoljno. Kako je n prost, $(a, n) = 1$, pa a ima inverz modulo n, i ima jedinstveni inverz b modulo n takav da $1 \leqslant b \leqslant n-1$. Međutim, ako je $b = 1$ imali bismo $1 \equiv_n ab \equiv_n a$, što nije tačno, i ako je $b = n-1$ imali bismo $1 \equiv_n ab \equiv_n -a$, što takođe nije tačno. Dakle, $2 \leqslant b \leqslant n-2$. Ostaje da dokažemo $b \neq a$. Ako je $a = b$ onda je $1 \equiv_n ab = a^2$, pa $n \mid a^2 - 1 = (a-1)(a+1)$. S obzirom da je n prost, $n \mid a-1$ ili $n \mid a+1$, odnosno $a \equiv_n \pm 1$, a znamo da to nije tačno.

Ako je broj b odgovara broju a kako je opisano u prethodnom pasusu, očigledno broj a odgovara broju b. Dakle, brojevi $2, \ldots, n-2$ zaista su podeljenji po parovima takvim da je proizvod svakog para jednak 1 modulo n. Prema tome i P je 1 modulo n. Konačno, $(n-1)! = 1 \cdot P \cdot (n-1) \equiv_n 1 \cdot 1 \cdot (-1) = -1$.

($\Leftarrow$) Neka n nije prost broj. Tada postoje m, k takvi da $1 < m, k < n$ i $n = mk$. Ako možemo da nađemo m i k tako da $m < k$, onda je $(n-1)! = 1 \cdots m \cdots k \cdots (n-1) \equiv_n 0$

jer je $(n-1)!$ očigledno umnožak od n. Kada različite m i k ne možemo da nađemo? Pa jedino kad je $m = k$ jedini delilac broja n za koji je $1 < m < n$. Brojevi koji imaju samo jedan pravi delilac su $n = p^2$ gde je p prost. Ako je $p = 2$, tj. $n = 4$, tada je $(4-1)! = 3! = 6 \equiv_4 2 \not\equiv_4 -1$. Ako je $p \geqslant 3$, onda se u $(n-1)! = (p^2-1)!$ javljaju činioci p i $2p$, pa je $(n-1)!$ umnožak od $p^2 = n$, tj. $(n-1)! \equiv_n 0 \not\equiv_n -1$. Ω