Elementarna teorija brojeva

Diskretne strukture s teorijom grafova

Damir Horvat

FOI, Varaždin

Relacija *dijeli* na skupu cijelih brojeva

$$a \mid b \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad \exists k \in \mathbb{Z},\ \ b = ak$$

Važno svojstvo relacije *dijeli*

$$a, b, c \in \mathbb{Z},\ \ (c \mid a) \wedge (c \mid b) \quad \Longrightarrow \quad c \mid k_1 a + k_2 b,\ \ \forall k_1, k_2 \in \mathbb{Z}$$

Zadatak 1

Dokažite da su prirodni brojevi n i $n+1$ relativno prosti.

Rješenje

$\boxed{\text{Tvrdimo}}$ $M(n, n+1) = 1$

Neka je $d = M(n, n+1)$.

$\boxed{d \in \mathbb{N}}$

$$d = M(n, n+1) \ \Rightarrow \ d \mid n,\ \ d \mid n+1 \ \Rightarrow$$

$$\Rightarrow \ d \mid 1 \cdot n + (-1) \cdot (n+1) \ \Rightarrow \ d \mid -1 \ \Rightarrow \ d = 1$$

$$a, b, c \in \mathbb{Z},\ \ (c \mid a) \wedge (c \mid b) \quad \Longrightarrow \quad c \mid k_1 a + k_2 b,\ \ \forall k_1, k_2 \in \mathbb{Z}$$

Zadatak 2

Odredite sve prirodne brojeve s kojima se može skratiti razlomak $\frac{5n+6}{8n+7}$ pri čemu je $n \in \mathbb{N}$.

Rješenje

Neka je $d = M(5n+6, 8n+7)$.

$$d = M(5n+6, 8n+7) \ \Rightarrow \ d \mid 5n+6,\ \ d \mid 8n+7 \ \Rightarrow$$

$$\Rightarrow \ d \mid 8 \cdot (5n+6) - 5 \cdot (8n+7) \ \Rightarrow \ d \mid 13 \ \Rightarrow \ d = 1 \text{ ili } d = 13$$

Dakle, razlomak $\frac{5n+6}{8n+7}$ se uopće ne može skratiti ili se može skratiti s brojem 13.

$$a, b, c \in \mathbb{Z},\ \ (c \mid a) \wedge (c \mid b) \quad \Longrightarrow \quad c \mid k_1 a + k_2 b,\ \ \forall k_1, k_2 \in \mathbb{Z}$$

$$a, b \in \mathbb{Z},\ b \neq 0 \implies \exists! q, r \in \mathbb{Z},\ a = bq + r,\ 0 \leqslant r < |b|$$

$$q = \begin{cases} \left\lfloor \dfrac{a}{b} \right\rfloor, & \text{ako je } b > 0 \\[2ex] \left\lceil \dfrac{a}{b} \right\rceil, & \text{ako je } b < 0 \end{cases}$$

$$r = a - bq$$

Zadatak 3

Odredite redukciju od 2015 i −2015 modulo 326.

Rješenje

- $2015 \mod 326 = 59 \rightsquigarrow 2015 \equiv 59 \pmod{326}$

$\lfloor x \rfloor$, $\lceil x \rceil$: 6, x, 7

$$q = \left\lfloor \frac{2015}{326} \right\rfloor = \lfloor 6.1809\cdots \rfloor = 6$$

$$r = 2015 - 326 \cdot 6 = 59$$

- $-2015 \mod 326 = 267 \rightsquigarrow -2015 \equiv 267 \pmod{326}$

$\lfloor x \rfloor$, $\lceil x \rceil$: -7, x, -6

$$q = \left\lfloor \frac{-2015}{326} \right\rfloor = \lfloor -6.1809\cdots \rfloor = -7$$

$$r = -2015 - 326 \cdot (-7) = 267$$

Zadatak 4

Odredite kvocijent i ostatak pri dijeljenju broja 3128 s brojem −219.

Rješenje

$$3128 = -219 \cdot q + r$$

$\lfloor x \rfloor$, $\lceil x \rceil$: -15, x, -14

$$q = \left\lceil \frac{3128}{-219} \right\rceil = \lceil -14.2831\cdots \rceil = -14$$

$$r = 3128 - (-219) \cdot (-14) = 62$$

Euklidov algoritam i prošireni Euklidov algoritam

Najveća zajednička mjera

$$\begin{aligned} a &= bq_1 + r_1, & 0 < r_1 < |b| \\ b &= r_1 q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2 \\ r_2 &= r_3 q_4 + r_4, & 0 < r_4 < r_3 \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k, & 0 < r_k < r_{k-1} \\ r_{k-1} &= r_k q_{k+1} \end{aligned}$$

$$M(a, b) = r_k$$

Cjelobrojno rješenje jednadžbe

$$ax + by = M(a, b), \quad a, b \in \mathbb{Z}$$

$$r_i = r_{i-2} - q_i r_{i-1},\ r_{-1} = a,\ r_0 = b$$
$$x_i = x_{i-2} - q_i x_{i-1},\ x_{-1} = 1,\ x_0 = 0$$
$$y_i = y_{i-2} - q_i y_{i-1},\ y_{-1} = 0,\ y_0 = 1$$

- Jedno cjelobrojno rješenje

$$x = x_k,\ y = y_k$$

$$ax_i + by_i = r_i, \quad i = -1, 0, 1, 2, \ldots, k, k+1$$

Zadatak 5

Odredite jedno cjelobrojno rješenje jednadžbe

$$28x + 2456y = M(28, 2456).$$

$$x_i = x_{i-2} - q_i x_{i-1}$$
$$y_i = y_{i-2} - q_i y_{i-1}$$

Rješenje 1. način $M(28, 2456) = 4$

$$\begin{aligned} 28 &= 2456 \cdot \boxed{0} + 28 \\ 2456 &= 28 \cdot \boxed{87} + 20 \\ 28 &= 20 \cdot \boxed{1} + 8 \\ 20 &= 8 \cdot \boxed{2} + \boxed{4} \\ 8 &= 4 \cdot 2 \end{aligned}$$

$x = -263$, $y = 3$

i	-1	0	1	2	3	4
q_i			0	87	1	2
x_i	1	0	1	-87	88	-263
y_i	0	1	0	1	-1	3

2. način

$$\begin{aligned} 2456 &= 28 \cdot \boxed{87} + 20 \\ 28 &= 20 \cdot \boxed{1} + 8 \\ 20 &= 8 \cdot \boxed{2} + \boxed{4} \\ 8 &= 4 \cdot 2 \end{aligned}$$

$x = -263$, $y = 3$

i	-1	0	1	2	3
q_i			87	1	2
y_i	1	0	1	-1	3
x_i	0	1	-87	88	-263

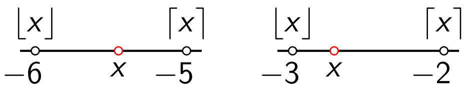
Zadatak 6

Odredite jedno cjelobrojno rješenje jednadžbe

$$2700x - 504y = M(2700, -504).$$

$$x_i = x_{i-2} - q_i x_{i-1}$$
$$y_i = y_{i-2} - q_i y_{i-1}$$

$M(2700, -504) = 36$



Rješenje

$$\begin{aligned} 2700 &= -504 \cdot \boxed{(-5)} + 180 \\ -504 &= 180 \cdot \boxed{(-3)} + \boxed{36} \\ 180 &= 36 \cdot 5 \end{aligned}$$

$$q_1 = \left\lceil \frac{2700}{-504} \right\rceil = \lceil -5.35\cdots \rceil = -5$$

$$r_1 = 2700 - (-504) \cdot (-5) = 180$$

$$q_2 = \left\lfloor \frac{-504}{180} \right\rfloor = \lfloor -2.8 \rfloor = -3$$

$$r_2 = -504 - 180 \cdot (-3) = 36$$

i	-1	0	1	2
q_i			-5	-3
x_i	1	0	1	3
y_i	0	1	5	16

$x = 3$ $y = 16$

Svojstva kongruencija

- Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, tada je

$$a + c \equiv b + d \pmod{n}$$
$$a - c \equiv b - d \pmod{n}$$
$$ac \equiv bd \pmod{n}$$

- Ako je $a \equiv b \pmod{n}$ i $d \mid n$, tada je $a \equiv b \pmod{d}$.
- Ako je $a \equiv b \pmod{n}$, tada je $ac \equiv bc \pmod{nc}$ za svaki $c \in \mathbb{N}$.
- Ako je $a \equiv b \pmod{n}$ i $f \in \mathbb{Z}[x]$, tada je $f(a) \equiv f(b) \pmod{n}$.
- Dijeljenje kongruencija

$$ax \equiv ay \pmod{n} \iff x \equiv y \left(\text{mod } \frac{n}{M(a,n)}\right)$$

Primjer

- Pretpostavimo da vrijedi $2a \equiv 11b \pmod{6}$.

$$11 \equiv 5 \pmod{6} \; / \cdot b$$
$$11b \equiv 5b \pmod{6}$$

- Tranzitivnost relacije *"biti kongruentan"*

$$2a \equiv 11b \pmod{6}, \; 11b \equiv 5b \pmod{6} \;\Rightarrow\; 2a \equiv 5b \pmod{6}$$

- Redukcija koeficijenata

$$2a \equiv \boxed{11}b \pmod{6} \iff 2a \equiv \boxed{5}b \pmod{6}$$

$$11 \equiv 5 \pmod{6}$$

Zadatak 7

Na skupu $\mathbb{Z}$ definirana je relacija $\sim$ s

$$a \sim b \overset{\text{def}}{\iff} 5 \mid 2a + 3b.$$

a) *Dokažite da je $\sim$ relacija ekvivalencije na skupu $\mathbb{Z}$.*

b) *Odredite klasu broja 1.*

c) *Odredite kvocijentni skup $\mathbb{Z}/\sim$.*

Rješenje

a) Treba provjeriti da je $\sim$ refleksivna, simetrična i tranzitivna relacija.

Refleksivnost $\quad (\forall a \in \mathbb{Z})(a \sim a)$

$$a \sim a \Leftrightarrow 5 \mid 2a + 3a \Leftrightarrow 5 \mid 5a$$

$a \sim b \overset{\text{def}}{\iff} 5 \mid 2a + 3b$

$5 \mid 2b + 3a$

Simetričnost $\quad (\forall a, b \in \mathbb{Z})(a \sim b \Rightarrow b \sim a)$

$$a \sim b \Rightarrow 5 \mid 2a + 3b \Rightarrow 2a + 3b \equiv 0 \pmod 5 \ /\cdot(-1) \Rightarrow$$

$-3 \equiv 2 \pmod 5$

$$\Rightarrow -2a - 3b \equiv 0 \pmod 5 \Rightarrow 3a + 2b \equiv 0 \pmod 5 \Rightarrow$$

$-2 \equiv 3 \pmod 5$

$$\Rightarrow 2b + 3a \equiv 0 \pmod 5 \Rightarrow 5 \mid 2b + 3a \Rightarrow b \sim a$$

$a \sim b \overset{\text{def}}{\iff} 5 \mid 2a + 3b$

$5 \mid 2a + 3c$

Tranzitivnost $\quad (\forall a, b, c \in \mathbb{Z})\big((a \sim b) \wedge (b \sim c) \Rightarrow a \sim c\big)$

$$(a \sim b) \wedge (b \sim c) \Rightarrow 5 \mid 2a + 3b \ \wedge \ 5 \mid 2b + 3c \Rightarrow$$

$$\Rightarrow 5 \mid (2a + 3b) + (2b + 3c) \Rightarrow 5 \mid 2a + 3c + 5b \Rightarrow$$

$$\Rightarrow 5 \mid 2a + 3c \Rightarrow a \sim c$$

$$a, b, c \in \mathbb{Z},\ (c \mid a) \wedge (c \mid b) \implies c \mid k_1 a + k_2 b,\ \forall k_1, k_2 \in \mathbb{Z}$$

$a \sim b \overset{\text{def}}{\iff} 5 \mid 2a + 3b$

b)

$$[1]_\sim = \{x \in \mathbb{Z} : x \sim 1\} = \{x \in \mathbb{Z} : 5 \mid 2x + 3 \cdot 1\} =$$

$$= \{x \in \mathbb{Z} : 5 \mid 2x + 3\} = \{x \in \mathbb{Z} : x \equiv 1 \pmod 5\} =$$

$$= 5\mathbb{Z} + 1$$

$-3 \equiv 2 \pmod 5$

$$5 \mid 2x + 3 \Leftrightarrow 2x + 3 \equiv 0 \pmod 5 \Leftrightarrow 2x \equiv -3 \pmod 5 \Leftrightarrow$$

$$\Leftrightarrow 2x \equiv 2 \pmod 5 \ /:2 \Leftrightarrow x \equiv 1 \pmod 5$$

$M(2,5) = 1$

$$ax \equiv ay \pmod n \iff x \equiv y \left(\mathrm{mod}\ \frac{n}{M(a,n)}\right)$$

$\boxed{a \sim b \overset{\text{def}}{\iff} 5 \mid 2a+3b}$

c) Tvrdimo da vrijedi

$$a \sim b \iff a \equiv b \pmod 5.$$

$$a \sim b \Leftrightarrow 5 \mid 2a+3b \Leftrightarrow 2a+3b \equiv 0 \pmod 5 \Leftrightarrow$$

$$\Leftrightarrow 2a \equiv \underset{\substack{\downarrow \\ -3 \equiv 2 \pmod 5}}{-3}b \pmod 5 \Leftrightarrow 2a \equiv 2b \pmod 5 \Leftrightarrow a \equiv b \pmod 5$$

$M(2,5)=1$

$$\mathbb{Z}/\!\sim\; = \{5\mathbb{Z},\, 5\mathbb{Z}+1,\, 5\mathbb{Z}+2,\, 5\mathbb{Z}+3,\, 5\mathbb{Z}+4\}$$

$$ax \equiv ay \pmod n \iff x \equiv y \left(\mathrm{mod}\ \frac{n}{M(a,n)}\right)$$

Teorem o rješenjima linearne kongruencije

Neka su $a, b \in \mathbb{Z}$, $a \neq 0$ i $n \in \mathbb{N} \setminus \{1\}$. Kongruencija

$$ax \equiv b \pmod n$$

ima rješenje akko $M(a,n) = d \mid b$. Ako je ovaj uvjet zadovoljen, tada gornja kongruencija ima d rješenja modulo n.

$$ax \equiv b \pmod n, \quad d = M(a,n)$$

$$a = a'd, \quad b = b'd, \quad n = n'd$$

$$ax \equiv b \pmod n \;/ : d$$

$$a'x \equiv b' \pmod{n'}$$

- $M(a', n') = 1$
- $a'x \equiv b' \pmod{n'}$ ima jedinstveno rješenje x_0 modulo n'.

Rješenja od $ax \equiv b \pmod n$

$$x_k = x_0 + kn', \; k = 0, 1, \ldots, d-1$$

Kako pronaći x_0?

$$M(a', n') = 1 \Rightarrow$$

$$\Rightarrow \exists u, v \in \mathbb{Z},\; a'u + n'v = 1 \Rightarrow$$

$$\Rightarrow 1 - a'u = n'v \Rightarrow$$

$$\Rightarrow n' \mid 1 - a'u \Rightarrow$$

$$\Rightarrow a'u \equiv 1 \pmod{n'} \;/ \cdot b' \Rightarrow$$

$$\Rightarrow a'(ub') \equiv b' \pmod{n'}$$

$$\boxed{x_0 = ub' \bmod n'}$$

<u>prošireni Euklidov algoritam</u>

početak: n' dijelimo s a'

$$u \rightsquigarrow y_i = y_{i-2} - q_i y_{i-1}$$

$$y_{-1} = 0, \; y_0 = 1$$

$$ax \equiv b \pmod n, \quad a'x \equiv b' \pmod{n'}, \quad a = a'd, \; b = b'd, \; n = n'd$$

$\boxed{M(a,n) = d}$

$$\begin{aligned} n &= aq_1 + r_1, & 0 < r_1 < a \\ a &= r_1 q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2 \\ &\vdots \end{aligned}$$

$\boxed{M(a',n') = 1}$

$$\begin{aligned} n' &= a'q_1 + r_1', & 0 < r_1' < a' \\ a' &= r_1' q_2 + r_2', & 0 < r_2' < r_1' \\ r_1' &= r_2' q_3 + r_3', & 0 < r_3' < r_2' \\ &\vdots \end{aligned}$$

$$n = aq_1 + r_1 \Rightarrow n'd = (a'd)q_1 + r_1 \;/ : d \Rightarrow n' = a'q_1 + \frac{r_1}{d} = r_1'$$

$$r_1' < a' \Leftrightarrow \frac{r_1}{d} < \frac{a}{d} \Leftrightarrow r_1 < a$$

$$a = r_1 q_2 + r_2 \Rightarrow a'd = (r_1'd)q_2 + r_2 \;/ : d \Rightarrow a' = r_1' q_2 + \frac{r_2}{d} = r_2'$$

$$r_2' < r_1' \Leftrightarrow \frac{r_2}{d} < \frac{r_1}{d} \Leftrightarrow r_2 < r_1$$

Zadatak 8

Riješite kongruenciju $4x \equiv 89 \pmod{527}$.

$$\boxed{\begin{aligned} a' &= a = 4 \\ b' &= b = 89 \\ n' &= n = 527 \end{aligned}}$$

Rješenje

$$\boxed{x_0 = ub' \bmod n'}$$

$$\begin{aligned} 527 &= 4 \cdot \overset{q_i}{\boxed{131}} + 3 \\ 4 &= 3 \cdot \boxed{1} + \boxed{1} \\ 3 &= 1 \cdot 3 \end{aligned}$$

$$\boxed{M(4, 527) = 1}$$

i	-1	0	1	2
q_i			131	1
y_i	0	1	-131	132

- Zadana kongruencija ima jedinstveno rješenje.

$$x_0 = 132 \cdot 89 \bmod 527 = 11\,748 \bmod 527 = 154$$

- Precizniji zapis rješenja $\boxed{x = 527k + 154,\ k \in \mathbb{Z}}$

$$x \equiv 154 \pmod{527}$$

Zadatak 9

$$\boxed{x_0 = ub' \bmod n'}$$

Riješite kongruenciju $234x \equiv 54 \pmod{5432}$.

Rješenje

$$\boxed{M(234, 5432) = 2}$$

$$\overset{a}{234}x \equiv \overset{b}{54} \pmod{\overset{n}{5432}} \ \big/ : 2$$

$$\overset{a'}{117}x \equiv \overset{b'}{27} \pmod{\overset{n'}{2716}}$$

$$\begin{aligned} 5432 &= 234 \cdot \overset{q_i}{\boxed{23}} + 50 \\ 234 &= 50 \cdot \boxed{4} + 34 \\ 50 &= 34 \cdot \boxed{1} + 16 \\ 34 &= 16 \cdot \boxed{2} + \boxed{2} \\ 16 &= 2 \cdot 8 \end{aligned}$$

i	-1	0	1	2	3	4
q_i			23	4	1	2
y_i	0	1	-23	93	-116	325

- $2 \mid 54 \longrightarrow$ kongruencija ima 2 rješenja

$$x_0 = 325 \cdot 27 \bmod 2716 = 8775 \bmod 2716 = 627$$

- Sva rješenja početne kongruencije: $x_k = x_0 + kn', \quad k = 0, 1$

$$x_k = 627 + 2716k, \quad k = 0, 1 \qquad \boxed{x_0 = 627} \qquad \boxed{x_1 = 3343}$$

Zadatak 10

$$\boxed{x_0 = ub' \bmod n'}$$

Riješite kongruenciju $21x \equiv 49 \pmod{2009}$.

Rješenje

$$\overset{a}{21}x \equiv \overset{b}{49} \pmod{\overset{n}{2009}} \ \big/ : 7$$

$$\overset{a'}{3}x \equiv \overset{b'}{7} \pmod{\overset{n'}{287}}$$

$$\begin{aligned} 2009 &= 21 \cdot \overset{q_i}{\boxed{95}} + 14 \\ 21 &= 14 \cdot \boxed{1} + \boxed{7} \\ 14 &= 7 \cdot 2 \end{aligned}$$

$$\boxed{M(21, 2009) = 7}$$

i	-1	0	1	2
q_i			95	1
y_i	0	1	-95	96

$$\boxed{\begin{aligned} x_0 &= 98 \\ x_1 &= 385 \\ x_2 &= 672 \\ x_3 &= 959 \\ x_4 &= 1246 \\ x_5 &= 1533 \\ x_6 &= 1820 \end{aligned}}$$

- $7 \mid 49 \longrightarrow$ kongruencija ima 7 rješenja

$$x_0 = 96 \cdot 7 \bmod 287 = 672 \bmod 287 = 98$$

- Sva rješenja početne kongruencije: $x_k = x_0 + kn', \quad k = 0, 1, \ldots, 6$

$$x_k = 98 + 287k, \quad k = 0, 1, \ldots, 6$$

Kineski teorem o ostacima

Neka su $n_1, n_2, \ldots, n_r$ u parovima relativno prosti prirodni brojevi, te neka su $a_1, a_2, \ldots, a_r$ cijeli brojevi. Tada sustav kongruencija

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

ima rješenje. Ako je x_0 jedno rješenje, tada su sva rješenja dana s

$$x \equiv x_0 \pmod{n_1 n_2 \cdots n_r}.$$

Zadatak 11

Riješite sustav kongruencija

$$x \equiv 1 \pmod{7}$$
$$x \equiv 5 \pmod{9}$$
$$x \equiv 3 \pmod{4}$$
$$x \equiv 9 \pmod{11}$$

$$396x_1 \equiv 1 \pmod{7} \qquad 308x_2 \equiv 5 \pmod{9}$$
$$4x_1 \equiv 1 \pmod{7} \qquad 2x_2 \equiv 5 \pmod{9}$$
$$\boxed{x_1 = 2} \qquad \boxed{x_2 = 7}$$
$$693x_3 \equiv 3 \pmod{4} \qquad 252x_4 \equiv 9 \pmod{11}$$
$$1 \cdot x_3 \equiv 3 \pmod{4} \qquad 10x_4 \equiv 9 \pmod{11}$$
$$\boxed{x_3 = 3} \qquad \boxed{x_4 = 2}$$

Rješenje

Moduli jesu u parovima relativno prosti.

$k_i x_i \equiv a_i \pmod{n_i}$

$$n = n_1 n_2 n_3 n_4 = 7 \cdot 9 \cdot 4 \cdot 11 = 2772$$

$$k_1 = \frac{n}{n_1} = 396, \quad k_2 = \frac{n}{n_2} = 308, \quad k_3 = \frac{n}{n_3} = 693, \quad k_4 = \frac{n}{n_4} = 252$$

$$x_0 = k_1 x_1 + k_2 x_2 + k_3 x_3 + k_4 x_4 \bmod n$$
$$x_0 = 396 \cdot 2 + 308 \cdot 7 + 693 \cdot 3 + 252 \cdot 2 \bmod 2772$$
$$x_0 = 5531 \bmod 2772 \qquad \boxed{x_0 = 2759} \qquad \boxed{x \equiv 2759 \pmod{2772}}$$

sva rješenja

Zadatak 12

Odredite sve prirodne brojeve između 900 i 999 koji pri dijeljenju s 4, 7 i 11 daju redom ostatke 3, 1 i 9.

$k_i x_i \equiv a_i \pmod{n_i}$

Rješenje

$$x \equiv 3 \pmod{4}$$
$$x \equiv 1 \pmod{7}$$
$$x \equiv 9 \pmod{11}$$

$$n = n_1 n_2 n_3 = 4 \cdot 7 \cdot 11 = 308$$

$$k_1 = \frac{n}{n_1} = 77, \quad k_2 = \frac{n}{n_2} = 44, \quad k_3 = \frac{n}{n_3} = 28$$

$$77x_1 \equiv 3 \pmod{4} \qquad 44x_2 \equiv 1 \pmod{7} \qquad 28x_3 \equiv 9 \pmod{11}$$
$$1 \cdot x_1 \equiv 3 \pmod{4} \qquad 2x_2 \equiv 1 \pmod{7} \qquad 6x_3 \equiv 9 \pmod{11}$$
$$\boxed{x_1 = 3} \qquad \boxed{x_2 = 4} \qquad \boxed{x_3 = 7}$$

$$x_0 = k_1 x_1 + k_2 x_2 + k_3 x_3 \bmod n$$
$$x_0 = 77 \cdot 3 + 44 \cdot 4 + 28 \cdot 7 \bmod 308$$
$$x_0 = 603 \bmod 308 \qquad \boxed{x_0 = 295} \qquad \boxed{x \equiv 295 \pmod{308}}$$

sva rješenja

$$x \equiv 295 \pmod{308}$$
$$x = 308k + 295, \ \ k \in \mathbb{Z}$$

$$900 \leqslant 308k + 295 \leqslant 999$$

$$308k + 295 \geqslant 900 \qquad\qquad 308k + 295 \leqslant 999$$
$$308k \geqslant 900 - 295 \qquad\qquad 308k \leqslant 999 - 295$$
$$308k \geqslant 605 \qquad\qquad 308k \leqslant 704$$
$$k \geqslant 1.96\cdots \qquad\qquad k \leqslant 2.28\cdots$$

$$1.96\cdots \leqslant k \leqslant 2.28\cdots$$
$$k = 2$$

$$x = 308 \cdot 2 + 295$$
$$\boxed{x = 911}$$

Zadatak 13

Riješite sustav kongruencija

$$7x \equiv 6 \pmod{15} \rightsquigarrow x \equiv 3 \pmod{15}$$
$$x \equiv 6 \pmod{12} \rightsquigarrow x \equiv 6 \pmod{12}$$
$$3x \equiv 1 \pmod{7} \rightsquigarrow x \equiv 5 \pmod{7}$$

Moduli nisu u parovima relativno prosti

Rješenje

Što ako neka od kongruencija ima više rješenja?

- Riješimo linearnu kongruenciju $7x \equiv 6 \pmod{15}$.

  $M(7,15) = 1 \longrightarrow$ kongruencija ima jedinstveno rješenje

  $x = 3$, tj. $x \equiv 3 \pmod{15}$

- Riješimo linearnu kongruenciju $3x \equiv 1 \pmod{7}$.

  $M(3,7) = 1 \longrightarrow$ kongruencija ima jedinstveno rješenje

  $x = 5$, tj. $x \equiv 5 \pmod{7}$

$$x \equiv 3 \pmod{15} \rightsquigarrow \begin{cases} x \equiv 3 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases} \rightsquigarrow \begin{cases} \boxed{x \equiv 0 \pmod{3}} \\ \boxed{x \equiv 3 \pmod{5}} \end{cases}$$

$$x \equiv 6 \pmod{12} \rightsquigarrow \begin{cases} x \equiv 6 \pmod{3} \\ x \equiv 6 \pmod{4} \end{cases} \rightsquigarrow \begin{cases} x \equiv 0 \pmod{3} \\ \boxed{x \equiv 2 \pmod{4}} \end{cases}$$

$$\boxed{x \equiv 5 \pmod{7}}$$

$$\begin{aligned} x &= 24k + 1 \\ &= 4 \cdot (6k) + 1 \\ &= 6 \cdot (4k) + 1 \end{aligned}$$

$$\begin{aligned} x &\equiv 0 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{4} \\ x &\equiv 5 \pmod{7} \end{aligned}$$

Moduli jesu u parovima relativno prosti

$$x \equiv 1 \pmod{24} \quad \Longrightarrow \quad x \equiv 1 \pmod{4},\ x \equiv 1 \pmod{6}$$
$$\not\Longleftarrow \quad \text{(protuprimjer: } x = 13\text{)}$$

$$\begin{aligned} x &\equiv 0 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{4} \\ x &\equiv 5 \pmod{7} \end{aligned}$$

$$k_i x_i \equiv a_i \pmod{n_i}$$

$$140x_1 \equiv 0 \pmod{3} \qquad 84x_2 \equiv 3 \pmod{5}$$
$$2x_1 \equiv 0 \pmod{3} \qquad 4x_2 \equiv 3 \pmod{5}$$
$$\boxed{x_1 = 0} \qquad \boxed{x_2 = 2}$$

$$105x_3 \equiv 2 \pmod{4} \qquad 60x_4 \equiv 5 \pmod{7}$$
$$1 \cdot x_3 \equiv 2 \pmod{4} \qquad 4x_4 \equiv 5 \pmod{7}$$
$$\boxed{x_3 = 2} \qquad \boxed{x_4 = 3}$$

$$n = n_1 n_2 n_3 n_4 = 3 \cdot 5 \cdot 4 \cdot 7 = 420$$

$$k_1 = \frac{n}{n_1} = 140, \quad k_2 = \frac{n}{n_2} = 84, \quad k_3 = \frac{n}{n_3} = 105, \quad k_4 = \frac{n}{n_4} = 60$$

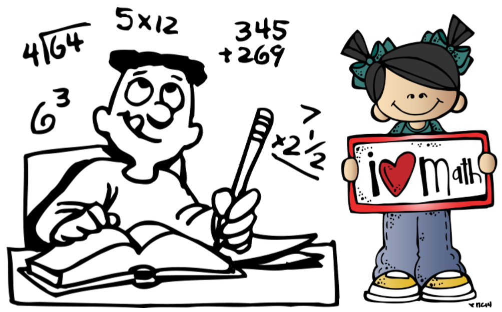
$$x_0 = k_1x_1 + k_2x_2 + k_3x_3 + k_4x_4 \bmod n$$
$$x_0 = 140 \cdot 0 + 84 \cdot 2 + 105 \cdot 2 + 60 \cdot 3 \bmod 420$$
$$x_0 = 558 \bmod 420 \qquad \boxed{x_0 = 138} \qquad \boxed{x \equiv 138 \pmod{420}}$$

sva rješenja

Domaća zadaća

Neka su $a, b \in \mathbb{N}$ takvi da je $M(a, b) = 1$ i $N \in \mathbb{Z}$. Dokažite da tada vrijedi:

$$x \equiv N \pmod{a},\ x \equiv N \pmod{b} \iff x \equiv N \pmod{ab}$$



Zadatak 14

Riješite sustav kongruencija

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{12} \\ x &\equiv 7 \pmod{14} \end{aligned}$$

$$\boxed{\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{3} \end{aligned}} \qquad \text{Kontradikcija}$$

$$\begin{aligned} x &\equiv 1 \pmod{4} \\ x &\equiv 0 \pmod{7} \end{aligned}$$

Rješenje

$$\boxed{x \equiv 2 \pmod{3}}$$

$$x \equiv 1 \pmod{12} \rightsquigarrow \begin{cases} \boxed{x \equiv 1 \pmod{3}} \\ \boxed{x \equiv 1 \pmod{4}} \end{cases} \rightsquigarrow \boxed{x \equiv 1 \pmod{4}}$$

$$x \equiv 7 \pmod{14} \rightsquigarrow \begin{cases} x \equiv 7 \pmod{2} \\ x \equiv 7 \pmod{7} \end{cases} \rightsquigarrow \begin{cases} \boxed{x \equiv 1 \pmod{2}} \\ \boxed{x \equiv 0 \pmod{7}} \end{cases}$$

$$\begin{aligned} x &= 4k + 1 \\ &= 2 \cdot (2k) + 1 \end{aligned}$$

Zadani sustav kongruencija nema rješenja.

Eulerova funkcija

$$\varphi : \mathbb{N} \to \mathbb{N}$$

- $\varphi(n)$ je jednak broju brojeva u nizu $1, 2, \ldots, n$ koji su relativno prosti s n
- φ je multiplikativna funkcija

$$\varphi(mn) = \varphi(m)\varphi(n), \quad m, n \in \mathbb{N}, \ M(m,n) = 1$$

- Ako je p prosti broj, tada za svaki $i \in \mathbb{N}$ vrijedi

$$\varphi(p^i) = p^i - p^{i-1}$$

- Ako je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ faktorizacija broja n na proste faktore, tada je

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Primjer

1. način

$M(25,4) = 1$

$\boxed{\varphi(p^i) = p^i - p^{i-1}}$

$$\varphi(100) = \varphi(25 \cdot 4) = \varphi(25) \cdot \varphi(4) = \varphi(5^2) \cdot \varphi(2^2) =$$

$$= (5^2 - 5^1) \cdot (2^2 - 2^1) = 20 \cdot 2 = 40$$

2. način

$$100 = 2^2 \cdot 5^2$$

$$\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

$$\boxed{\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)}$$

Usporedba

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\varphi(n) = \boxed{n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)} =$$

$$= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) =$$

$$= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) =$$

$$= \boxed{\left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right)} =$$

$$= \varphi\left(p_1^{\alpha_1}\right) \cdot \varphi\left(p_2^{\alpha_2}\right) \cdots \varphi\left(p_k^{\alpha_k}\right)$$

Eulerov teorem

Ako je $M(a,n) = 1$, tada je $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Mali Fermatov teorem

Neka je p prosti broj. Ako $p \nmid a$, tada je

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

Nadalje, za svaki $a \in \mathbb{Z}$ vrijedi $a^p \equiv a \pmod{p}$.

- Obrat malog Fermatovog teorema ne vrijedi.
- Protuprimjer su **Carmichaelovi brojevi**.
- Najmanji Carmichaelov broj je 561.

Zadatak 15

Dokažite da je 137 prosti broj i odredite ostatak pri dijeljenju broja 26^{282} s brojem 137.

Rješenje

$\sqrt{137} \approx 11.7047 \qquad 2,3,5,7,11$

Niti jedan od prostih brojeva $2,3,5,7,11$ nije faktor od 137 pa zaključujemo da je 137 prosti broj.

$\boxed{\text{Mali Fermatov teorem}}$ $M(26,137)=1 \;\Rightarrow\; 26^{137-1} \equiv 1 \pmod{137}$

$$26^{136} \equiv 1 \pmod{137} \;/^{2}$$
$$\boxed{\begin{aligned} 26^{272} &\equiv 1 \pmod{137} \\ 26^{10} &\equiv 135 \pmod{137} \end{aligned}} \;/\cdot$$
$$\boxed{26^{282} \equiv 135 \pmod{137}}$$

$$26^{3} \equiv 40 \pmod{137} \;/^{3}$$
$$26^{9} \equiv 40^{3} \pmod{137}$$
$$26^{9} \equiv 21 \pmod{137} \;/\cdot 26$$
$$26^{10} \equiv 546 \pmod{137}$$

RSA kriptosustav

- $n = pq, \quad p$ i q su pažljivo odabrani veliki prosti brojevi
- $\varphi(n) = (p-1)(q-1)$
- biramo $e \in \mathbb{N}, \quad 1 < e < \varphi(n), \quad M(e,\varphi(n)) = 1$
- $d \in \mathbb{N}$ je rješenje kongruencije $de \equiv 1 \pmod{\varphi(n)}$
- $\boxed{\text{javni dio ključa}}$ (n,e) $\qquad$ $\boxed{\text{tajni dio ključa}}$ (p,q,d)
- $\boxed{\text{šifriranje}}$ $E(x) = x^{e} \mod n$
- $\boxed{\text{dešifriranje}}$ $D(y) = y^{d} \mod n$
- $\boxed{\text{digitalni potpis}}$ $S_B(x) = D_B(E_A(x))$

$$\text{Bob} \xrightarrow{(E_A(x),\, S_B(x))} \text{Alice}$$

Zadatak 16

$\boxed{\varphi(100) = 40}$

Odredite zadnje dvije znamenke broja $3^{501} \cdot 7^{200}$.

Rješenje

$\boxed{\text{Zadnje dvije znamenke broja } 3^{501} \cdot 7^{200} \text{ su } 03.}$

Zanima nas ostatak pri dijeljenju broja $3^{501} \cdot 7^{200}$ s brojem 100.

$\boxed{\text{Eulerov teorem}}$ $M(3,100)=1 \;\Rightarrow\; 3^{\varphi(100)} \equiv 1 \pmod{100}$

$\boxed{\text{Eulerov teorem}}$ $M(7,100)=1 \;\Rightarrow\; 7^{\varphi(100)} \equiv 1 \pmod{100}$

$$3^{40} \equiv 1 \pmod{100} \;/^{12}$$
$$\boxed{\begin{aligned} 3^{480} &\equiv 1 \pmod{100} \\ 3^{21} &\equiv 3 \pmod{100} \end{aligned}} \;/\cdot$$
$$\boxed{\begin{aligned} 3^{501} &\equiv 3 \pmod{100} \\ 7^{200} &\equiv 1 \pmod{100} \end{aligned}} \;/\cdot$$

$$3^{10} \equiv 49 \pmod{100} \;/^{2}$$
$$3^{20} \equiv 49^{2} \pmod{100}$$
$$3^{20} \equiv 1 \pmod{100} \;/\cdot 3$$
$$7^{40} \equiv 1 \pmod{100} \;/^{5}$$
$$\boxed{3^{501} \cdot 7^{200} \equiv 3 \pmod{100}}$$

Zadatak 17

$\boxed{E(x) = x^{e} \mod n}$

Javni RSA ključ od Alice je $(n_A, e_A) = (221, 5)$.

a) *Šifrirajte za Alice poruku $x = 10$.*

b) *Odredite tajni RSA ključ koji pripada javnom ključu od Alice.*

c) *Bob je primio šifriranu poruku $y = 172$ i uz nju potpis $S = 144$. Je li poruku poslala Alice?*

Rješenje

a)

$$y = x^{e_A} \mod n_A$$
$$y = 10^{5} \mod 221$$
$$y = 100\,000 \mod 221$$
$$y = 108$$

$$q = \left\lfloor \frac{100\,000}{221} \right\rfloor = \lfloor 452.4886\cdots \rfloor$$
$$q = 452$$
$$r = 100\,000 - 221 \cdot 452$$
$$r = 108$$

$x_0 = ub' \mod n'$

$(n_A, e_A) = (221, 5)$

b)

$$221 = \overset{p}{13} \cdot \overset{q}{17}$$

$$\varphi(221) = \varphi(13) \cdot \varphi(17) = 12 \cdot 16 = 192$$

$$ed \equiv 1 \pmod{\varphi(n)}$$

$$5d \equiv 1 \pmod{192}$$

$$\begin{aligned} 192 &= 5 \cdot \overset{q_i}{\boxed{38}} + 2 \\ 5 &= 2 \cdot \boxed{2} + \boxed{1} \\ 2 &= 1 \cdot 2 \end{aligned}$$

$M(5, 192) = 1$

i	-1	0	1	2
q_i			38	2
y_i	0	1	-38	77

$$d = 77 \cdot 1 \mod 192$$

$$d = 77$$

Tajni RSA ključ od Alice $(p, q, d) = (13, 17, 77)$

c)

Poruku nije poslala Alice.

$(n_A, e_A) = (221, 5)$

$$\text{Alice} \xrightarrow{(E_B(x),\ S_A(x))} \text{Bob}$$

$$S_A(x) = D_A(E_B(x)), \quad y = E_B(x) = 172, \quad S = 144$$

Alice je poslala poruku jedino ako je $E_A(S) = y$.

$$E_A(144) = 144^5 \mod 221 = 196 \neq 172$$

$$144^2 \equiv 183 \pmod{221} \ /^2$$

$$144^4 \equiv 33\,489 \pmod{221}$$

$$144^4 \equiv 118 \pmod{221} \ / \cdot 144$$

$$144^5 \equiv 16\,992 \pmod{221}$$

$$144^5 \equiv 196 \pmod{221}$$

$d = 77$ $(n_A, e_A) = (221, 5)$

Kako bi izgledao potpis da je Alice poslala poruku?

$$\text{Alice} \xrightarrow{(E_B(x),\ S_A(x))} \text{Bob}$$

$$S_A(x) = D_A(E_B(x)), \quad y = E_B(x) = 172$$

$$S_A(x) = D_A(y) = D_A(172) = 172^{77} \mod 221 = 100$$

Modularno potenciranje (binarna metoda)

Potenciranje – binarna metoda

$$x^y = x^{\sum\limits_{i=0}^{D-1} y_i 2^i} = \prod_{i=0}^{D-1} x^{y_i 2^i} = \prod_{i=0}^{D-1} \left(x^{2^i}\right)^{y_i}$$

- $x, y \in \mathbb{N}$
- $y_i \in \{0, 1\}, \ i = 0, 1, \ldots, D-1$
- Složenost potenciranja klasičnim načinom je $O(y)$.
- Složenost potenciranja binarnom metodom je $O(\log y)$.
- Na primjer, ako je $y = 2^{30}$, tada je broj množenja
  - kod klasičnog potenciranja reda veličine 1 073 741 824
  - kod binarne metode reda veličine 30

Primjer: $y = 13$

$$x^{13} = x^{(1101)_2} = x^{1\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0} =$$

$$= x^{2^0} \cdot x^{2^2} \cdot x^{2^3} = x \cdot x^4 \cdot x^8$$

$$x \xrightarrow{\text{kvadriraj}} x^2 \xrightarrow{\text{kvadriraj}} x^4 \xrightarrow{\text{kvadriraj}} x^8$$

$$1 \xrightarrow{\cdot x} x \xrightarrow{\cdot x^4} x^5 \xrightarrow{\cdot x^8} x^{13}$$

Algoritam: Modularno potenciranje – binarna metoda s desna na lijevo

Ulaz: $x, y, n \in \mathbb{N},\ y = (y_{D-1} \cdots y_1 y_0)_2$

Izlaz: $x^y \mod n$

$z := x \mod n$;

$a := 1$;

for $0 \leqslant j < D - 1$ **do**

  if $y_j = 1$ **then**

    $a := az \mod n$;

  end

  $z := z^2 \mod n$;

end

$a := az \pmod n$;

return a

$$77 = (\overset{y_6}{1}\ \overset{y_5}{0}\ \overset{y_4}{0}\ \overset{y_3}{1}\ \overset{y_2}{1}\ \overset{y_1}{0}\ \overset{y_0}{1})_2$$

$172^{77} \mod 221 = 100$

korak	a	z
0	1	172
1	172	191
2	172	16
3	100	35
4	185	120
5	185	35
6	185	120
7	$\boxed{100}$	–

0. korak

$a := 1$

$z := x \mod n$

$z := 172 \mod 221$

$z := 172$

1. korak $y_0 = 1$

$a := az \mod n$

$a := 1 \cdot 172 \mod 221$

$a := 172$

$z := z^2 \mod n$

$z := 172^2 \mod 221$

$z := 191$

2. korak $y_1 = 0$

$a := 172$

$z := z^2 \mod n$

$z := 191^2 \mod 221$

$z := 16$

3. korak $y_2 = 1$

$a := az \mod n$

$a := 172 \cdot 16 \mod 221$

$a := 100$

$z := z^2 \mod n$

$z := 16^2 \mod 221$

$z := 35$

4. korak $y_3 = 1$

$a := az \mod n$

$a := 100 \cdot 35 \mod 221$

$a := 185$

$z := z^2 \mod n$

$z := 35^2 \mod 221$

$z := 120$

5. korak $y_4 = 0$

$a := 185$

$z := z^2 \mod n$

$z := 120^2 \mod 221$

$z := 35$

6. korak $y_5 = 0$

$a := 185$

$z := z^2 \mod n$

$z := 35^2 \mod 221$

$z := 120$

7. korak $y_6 = 1$

$a := az \mod n$

$a := 185 \cdot 120 \mod 221$

$a := 100$

RSA u stvarnoj primjeni

Generiranje velikih prostih brojeva

- Generiramo slučajni broj s n bitova i na njega primijenimo neki vjerojatnosni test za ispitivanje prostosti (Eulerov kriterij, Miller-Rabinov test, ...).
- Ako broj ne prođe test, tada generiramo novi slučajni broj s n bitova i ponovimo postupak.
- Postupak ponavljamo tako dugo dok ne dobijemo prosti broj.
- Zahvaljujući teoremu o prostim brojevima nakon razumnog broja koraka dobit ćemo prosti broj.

$$\pi(x) \sim \frac{x}{\ln x}$$

RSA u stvarnoj primjeni

Množenje velikih prirodnih brojeva

- Složenost *školskog množenja* dva n-znamenkasta prirodna broja jednaka je $O(n^2)$.
- *Školsko množenje* nije efikasno na brojevima sa stotinjak i više znamenaka.
- Postoje razni moderni algoritmi za brzo množenje jako velikih prirodnih brojeva.

RSA u stvarnoj primjeni

- Jedna ideja je da se veliki prirodni brojevi podijele na manje dijelove, manji dijelovi se pomnože *školskim množenjem*, a nakon toga se spoje u cjelinu da se dobije traženi produkt.

Karatsubina metoda

- Svaki od brojeva se podijeli na dva jednaka dijela, manji dijelovi se na odgovarajući način *školski* pomnože i zatim spoje u cjelinu.
- Složenost je $O(n^{\log_2 3}) = O(n^{1.585})$ pri čemu je n broj znamenaka.
- Metoda je pogodna za brojeve sa stotinjak znamenaka.

RSA u stvarnoj primjeni

Toom-Cook metoda

- Poopćenje Karatsubine metode, brojevi se dijele na više manjih dijelova, a množenje brojeva se povezuje s množenjem polinoma.
- Polinomi se evaluiraju u određenom broju točaka tako da se dobije dovoljno podataka za njihov produkt. Tu se koristi *školsko množenje* manjih brojeva.
- Na temelju tih podataka rješavanjem sustava linearnih jednadžbi dobivaju se koeficijenti produkta dva polinoma iz kojih se dobije traženi produkt prirodnih brojeva. Rješavanje sustava se svodi na množenje matrice i vektora pri čemu opet množimo i zbrajamo manje brojeve.

RSA u stvarnoj primjeni

Toom-Cook metoda

- Složenost je $O(n^{1+\varepsilon})$ pri čemu je n broj znamenaka. Za dovoljno veliki stupanj polinoma, $\varepsilon > 0$ može biti proizvoljno blizu nule.
- Međutim, to je samo teorijska složenost jer u ovoj složenosti nisu brojana zbrajanja i množenja konstantama koja znatno rastu s povećanjem stupnja polinoma.

RSA u stvarnoj primjeni

Diskretna Fourierova transformacija

- Množenje prirodnih brojeva se temelji na diskretnoj Fourierovoj transformaciji signala i povezanosti množenja prirodnih brojeva s acikličkom konvolucijom signala.
- FFT algoritam (*Fast Fourier Transform*) je efikasan algoritam koji daje diskretnu Fourierovu transformaciju signala. Složenost mu je $O(D \ln D)$ pri čemu je D duljina signala.
- Množenje prirodnih brojeva se temelji na teoremu o konvoluciji, a složenost je jednaka $O(n \cdot \ln n \cdot \ln(\ln n))$ pri čemu je n broj znamenaka (bitova).

RSA u stvarnoj primjeni

Diskretna Fourierova transformacija

- Prirodni brojevi se poistovjete sa signalima i pronađe se diskretna Fourirerova transformacija oba signala preko FFT algoritma.
- Transformirani signali se pomnože po komponentama i pronađe se inverzna diskretna Fourierova transformacija tog produkta ponovo pomoću FFT algoritma.
- Napravimo zaokruživanje dobivenog signala na cijele brojeve, a komponente tog signala daju traženi produkt prirodnih brojeva (uz dodatno napravljeni prijenos znamenaka).
- Ovdje ulazimo u aritmetiku realnih brojeva pa treba paziti na preciznost da kod zaokruživanja ne dobijemo pogrešni rezultat.

RSA u stvarnoj primjeni

Modularno potenciranje

$x^y \mod n$

- Šifriranje i dešifriranje u RSA algoritmu je također efikasno.
- Postoje efikasni algoritmi za modularno potenciranje.
- Jedna od tih metoda je binarna metoda čija složenost je $O(\log y)$.
- Druga dobra metoda se temelji na **Montgomerijevom produktu**.

RSA u stvarnoj primjeni

Montgomerijevo potenciranje $x^y \mod n$

- Ideja Montgomerijevog potenciranja je izbjegavanje dijeljenja s modulom n.
- Modularno potenciranje se zapravo ne obavlja u klasičnom potpunom sustavu ostataka modulo n, već u transformiranom potpunom sustavu ostataka modulo n.
- U transformiranom sustavu ostataka se primijenjuje Montgomerijev produkt koji se u svakom koraku obavlja sa svega dva množenja.