Osječki matematički list 25 (2025), 31–49

Modularno potenciranje

Bernadin Ibrahimpašić*, Šejla Jusić†

Sažetak

U članku se opisuju osnovni pojmovi modularne aritmetike, tj. aritmetike u skupu $\mathbb{Z}_m$ koji predstavlja skup svih ostataka pri dijeljenju s prirodnim brojem m, s posebnim naglaskom na modularno potenciranje.

Ključne riječi: *kongruencije, modularna aritmetika, modularno potenciranje*

Modular exponentiation

Abstract

In this paper, we present the basic concepts of modular arithmetic, with special emphasis on modular exponentiation.

Keywords: *congruences, modular arithmetic, modular exponentiation*

*Pedagoški fakultet, Univerzitet u Bihaću, email: bernadin@bih.net.ba
†Pedagoški fakultet, Univerzitet u Bihaću, email: sejlaa.jusic@gmail.com

1 Djeljivost

Teorija brojeva je, pored geometrije, jedna od najstarijih grana matematike. Bavi se proučavanjem svojstava cijelih brojeva, s posebnim osvrtom na svojstva prirodnih brojeva. Jedan od glavnih ciljeva joj je otkrivanje zanimljivih i neočekivanih odnosa između različitih vrsta brojeva i dokazivanje istinitosti tvrdnji kojima se ti odnosi iskazuju. Carl Friedrich Gauss (1777 – 1855) je matematiku nazvao kraljicom znanosti a teoriju brojeva kraljicom matematike. On je 1801. godine, u svom djelu *Disquisitiones Arithmeticae*, koje se sastoji od 7 poglavlja, od kojih je prvih šest bilo posvećeno teoriji brojeva, uveo pojam kongruencije, poznat i pod nazivom modularna aritmetika.

Jedan od osnovnih pojmova u teoriji brojeva je pojam djeljivosti.

Definicija 1.1. *Neka su $m \neq 0$ i a cijeli brojevi. Kažemo da je a **djeljiv** s m, odnosno da m **dijeli** a, ako postoji cijeli broj q takav da je $a = mq$. To zapisujemo s $m|a$. Ako a nije djeljiv s m, onda pišemo $m \nmid a$.*

*Ako $m|a$, onda još kažemo da je m **djelitelj** ili **faktor** od a, a da je a **višekratnik** od m.*

Za prirodni broj n brojevi 1 i n nazivaju se njegovi **trivijalni djelitelji**, dok se njegov djelitelj d, takav da je $1 < d < n$, naziva **netrivijalni djelitelj** broja n. Pozitivan djelitelj broja n, koji je različit od n, naziva se **pravi djelitelj** broja n.

Relacija "biti djeljiv" je relacija parcijalnog uređaja na skupu prirodnih brojeva $\mathbb{N}$. To znači da za sve prirodne brojeve k, m i n vrijedi:

1. $m|m$ – refleksivnost,
2. $(k|m \wedge m|n) \implies k|n$ – tranzitivnost,
3. $(m|n \wedge n|m) \implies m = n$ – antisimetričnost.

Međutim, to nije relacija parcijalnog uređaja na skupu cijelih brojeva $\mathbb{Z}$, jer $m|n$ i $n|m \implies m = \pm n$ pa nije zadovoljena antisimetričnost.

Teorem 1.1 (Teorem o dijeljenju s ostatkom, [1, Teorem 2.2.]). *Za proizvoljan prirodni broj m i cijeli broj a postoje jedinstveni cijeli brojevi q i r takvi da je $a = mq + r$, $0 \leq r < m$. Broj q zove se **količnik**, a r **ostatak** pri dijeljenju broja a brojem m.*

Ostatak r često se označava i s $r = a \bmod m$, a može se definirati i kao

$$r = a - m \cdot \left\lfloor \frac{a}{m} \right\rfloor,$$

gdje $\lfloor x \rfloor$ predstavlja funkciju **najveće cijelo**, koja realnom broju x pridružuje najveći cijeli broj koji je manji ili jednak x. Govorimo o binarnoj operaciji mod m.

Na primjer, $23 \bmod 7 = 2$, jer je $23 = 3 \cdot 7 + 2$, dok je $-23 \bmod 7 = 5$, jer je $-23 = -4 \cdot 7 + 5$.

Neka svojstva binarne operacije mod m, koja slijede iz svojstava ostatka r (Teorem 1.1) te definicije i svojstava zbrajanja i množenja u skupu $\mathbb{Z}_m$ (Poglavlje 3), su sljedeća:

1. $(a \bmod m) \bmod m = a \bmod m$,
2. $m^k \bmod m = 0, \forall k \in \mathbb{N}$,
3. $ab^{p-1} \bmod p = a \bmod p, \forall p$ prost, $p \nmid b$,
4. $[(-a \bmod m) + (a \bmod m)] \bmod m = 0$,
5. $[(a^{-1} \bmod m)(a \bmod m)] \bmod m = 1$,
6. $(a + b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m$,
7. $ab \bmod m = [(a \bmod m)(b \bmod m)] \bmod m$,
8. $\frac{a}{b} \bmod m = [(a \bmod m)(b^{-1} \bmod m)] \bmod m$,
9. $[(ab \bmod m)(b^{-1} \bmod m)] \bmod m = a \bmod m$.

2 Kongruencije

Uz pojam djeljivosti direktno je vezan i pojam kongruencija. Definirat ćemo relaciju "biti kongruentan modulo m" i navesti neka njena svojstva.

Definicija 2.1. *Ako cijeli broj $m \neq 0$ dijeli razliku $a - b$, onda kažemo da je a **kongruentan** b modulo m i pišemo $a \equiv b \pmod{m}$. U protivnom kažemo da a **nije kongruentan** b modulo m i pišemo $a \not\equiv b \pmod{m}$.*

Na primjer, $17 \equiv 8 \pmod 9$, jer 9 dijeli razliku $17 - 8 = 9$ i $-23 \equiv 4 \pmod 9$, jer 9 dijeli razliku $-23 - 4 = -27$, ali $13 \not\equiv 5 \pmod 9$, jer 9 ne dijeli razliku $13 - 5 = 8$.

Kako je razlika $a - b$, $a, b \in \mathbb{Z}$, djeljiva s $-m$ ako i samo ako je djeljiva s m, to bez smanjenja općenitosti možemo promatrati samo slučajeve kada je m prirodni broj.

Također je razlika $a - b$ djeljiva s 1 za svaki $a, b \in \mathbb{Z}$, pa je svaki cijeli broj a kongruentan sa svakim cijelim brojem b modulo 1. Kongruenciju

modulo 1 nazivamo **trivijalna kongruencija**, pa možemo promatrati samo slučajeve kada je $m > 1$.

Na osnovu Definicije 2.1 zaključujemo da je $a \equiv b \pmod{m}$ ako i samo ako postoji $k \in \mathbb{Z}$ takav da je $a = km + b$. Tako je $17 \equiv 8 \pmod{9}$, jer je $17 = 1 \cdot 9 + 8$.

Za razliku od binarne operacije mod m, relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu cijelih brojeva $\mathbb{Z}$. To znači da za sve cijele brojeve a, b i c te prirodni broj m vrijedi:

1. $a \equiv a \pmod{m}$ – refleksivnost,
2. $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ – simetričnost,
3. $(a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$ – tranzitivnost.

Kako je relacija "biti kongruentan modulo m" relacija ekvivalencije na skupu $\mathbb{Z}$, to ona taj skup "razbija" na klase ekvivalencije, tj. na **klase kongruencije** ili **klase ostataka**. U svakoj toj klasi nalaze se oni i samo oni cijeli brojevi koji pri dijeljenju brojem m daju isti ostatak, tj. oni koji su kongruentni modulo m. Za predstavnika svake klase obično se uzima njen najmanji nenegativni element.

Jasno je da za sve cijele brojeve a i b te prirodni broj m vrijedi da je

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m.$$

Također, za sve cijele brojeve a, b, c i d te prirodne brojeve m i n, takve da je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$ vrijedi:

1. $a \pm c \equiv b \pm d \pmod{m}$,
2. $ac \equiv bd \pmod{m}$,
3. $a^n \equiv b^n \pmod{m}$.

Kao direktnu posljedicu navedenih svojstava dobivamo:

$$a \equiv b \pmod{m} \implies f(a) \equiv f(b) \pmod{m},$$

za svaki polinom f s cjelobrojnim koeficijentima.

Istaknimo još da je $ax \equiv ay \pmod{m}$ ako i samo ako je $x \equiv y \pmod{\frac{m}{\mathrm{nzd}(a,m)}}$. Specijalno, ako je $ax \equiv ay \pmod{m}$ i $\mathrm{nzd}(a, m) = 1$, onda je $x \equiv y \pmod{m}$. (vidjeti [1, Teorem 3.4.])

Primjer 2.1. *Odredimo posljednju znamenku broja* 7^{2023}.

Rješenje. Da bi se odredila posljednja znamenka broja 7^{2023} potrebno je odrediti ostatak pri dijeljenju broja 7^{2023} s brojem 10, tj. izračunati koliko iznosi 7^{2023} kongruentno modulo 10. Kako vrijedi

$$7^1 \equiv 7 \pmod{10}, \qquad 7^2 \equiv 49 \equiv 9 \pmod{10},$$
$$7^3 \equiv 63 \equiv 3 \pmod{10}, \quad 7^4 \equiv 21 \equiv 1 \pmod{10},$$

to je

$$7^{2023} = 7^{4\cdot 505+3} = (7^4)^{505} \cdot 7^3 \equiv 1^{505} \cdot 3 \equiv 3 \pmod{10}.$$

Dakle, posljednja znamenka broja 7^{2023} je 3. ◀

Primjer 2.2. *Nađimo ostatak pri dijeljenju sume* $1! + 2! + 3! + \cdots + 100!$ *s* 15.

Rješenje. Kako je $5! = 120 \equiv 0 \pmod{15}$, to je $k! \equiv 0 \pmod{15}$ za svaki $k \geq 5$ pa vrijedi

$$\begin{aligned} 1! + 2! + 3! + \cdots + 100! &\equiv 1! + 2! + 3! + 4! + 0 + \cdots + 0 \\ &\equiv 1 + 2 + 6 + 24 \equiv 33 \equiv 3 \pmod{15}. \end{aligned}$$

Dobili smo da je ostatak pri dijeljenju zadane sume s 15 jednak 3. ◀

3 Modularna aritmetika

Pojam modularne aritmetike je povezan s pojmom ostataka pri dijeljenju cijelog broja prirodnim. Primjenu je našla u teoriji brojeva, teoriji grupa, apstraktnoj algebri, kriptografiji, računarstvu te vizualnim umjetnostima i glazbi. Klasična, svakodnevna, primjena modularne aritmetike je prilikom računanja vremena, kada se radi o aritmetici modulo 24 (ili modulo 12).

Pri dijeljenju bilo kojeg cijelog broja prirodnim brojem m dobivamo jedan od ostataka $0, 1, 2, \ldots, m-1$. Skup svih ostataka pri dijeljenju cijelih brojeva prirodnim brojem m označavamo sa $\mathbb{Z}_m$, tj. imamo da je

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Na skupu $\mathbb{Z}_m$, operacije zbrajanja, u oznaci $+_m$, i množenja, u oznaci $\cdot_m$, tzv. operacije **modularnog zbrajanja** i **modularnog množenja**, se definiraju kao i standardno zbrajanje i množenje u skupu $\mathbb{Z}$, s tim da se, na kraju, za rezultat uzima ostatak pri dijeljenju s m. Dakle

$$a +_m b = (a + b) \bmod m \qquad \text{i} \qquad a \cdot_m b = (a \cdot b) \bmod m.$$

Modularno oduzimanje, u oznaci $-_m$, definira se analogno kao

$$a -_m b = (a - b) \bmod m,$$

ili kao zbrajanje sa suprotnim elementom, tj. kao

$$a -_m b = a +_m (-b \bmod m) = (a + (-b \bmod m)) \bmod m.$$

Primjer 3.1. *U skupu* $\mathbb{Z}_{31}$ *izračunajmo* $29 +_{31} 17$, $21 -_{31} 30$ *i* $11 \cdot_{31} 7$.

Rješenje.

$$\begin{aligned} 29 +_{31} 17 &= (29 + 17) \bmod 31 = 46 \bmod 31 = 15, \\ 21 -_{31} 30 &= (21 - 30) \bmod 31 = -9 \bmod 31 = 22, \\ 11 \cdot_{31} 7 &= (11 \cdot 7) \bmod 31 = 77 \bmod 31 = 15. \end{aligned}$$

◀

Napomenimo da su zbrajanje i oduzimanje u $\mathbb{Z}_m$ vrlo jednostavne operacije te uzimajući da su $x, y \in \mathbb{Z}_m$, možemo ih prikazati na način:

$$\begin{aligned} x +_m y &= \begin{cases} x + y \ , & x + y < m, \\ x + y - m \, , & x + y \geq m, \end{cases} \\ x -_m y &= \begin{cases} x - y \ , & x \geq y, \\ x - y + m \, , & x < y. \end{cases} \end{aligned}$$

Za razliku od zbrajanja i oduzimanja, množenje u $\mathbb{Z}_m$ nije tako jednostavno, jer pored standardnog množenja uključuje i modularnu redukciju, tj. dijeljenje.

Bitno je istaknuti da skup $\mathbb{Z}_m$, uz operacije modularnog zbrajanja i množenja, čini algebarsku strukturu prstena. Dakle, za svaki prirodni broj m i za sve $a, b, c \in \mathbb{Z}_m$ vrijedi:

1. $a +_m b, a \cdot_m b \in \mathbb{Z}_m$,
2. $(a +_m b) +_m c = a +_m (b +_m c)$ i $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$,
3. $a +_m b = b +_m a$ i $a \cdot_m b = b \cdot_m a$,
4. $a +_m 0 = 0 +_m a = a$,
5. $a \cdot_m 1 = 1 \cdot_m a = a$,
6. $a +_m (m - a) = (m - a) +_m a = 0$,
7. $a \cdot_m (b +_m c) = a \cdot_m b +_m a \cdot_m c$ i $(a +_m b) \cdot_m c = a \cdot_m c +_m b \cdot_m c$.

Definicija 3.1. ***Multiplikativni inverz*** *cijelog broja a modulo m je broj $a^{-1} \in \mathbb{Z}_m$ za koji vrijedi $aa^{-1} \equiv 1 \pmod{m}$.*

Kako ([1, Teorem 3.6.]) linearna kongruencija $ax \equiv b \pmod{m}$, gdje su a i m prirodni brojevi, te b cijeli broj, ima rješenje ako i samo ako $\text{nzd}(a, m)$ dijeli b, to vidimo da multiplikativni inverz broja a modulo m postoji ako i samo ako su a i m relativno prosti brojevi. Od posebnog je interesa kada je modul prost broj p, jer tada svaki nenulti element iz $\mathbb{Z}_p$ ima svoj multiplikativni inverz. Ako je p prost broj, tada je skup $\mathbb{Z}_p$, s operacijama modularnog zbrajanja i množenja, polje ([3, str. 138]).

Podijeliti element a elementom b u skupu $\mathbb{Z}_m$ znači pomnožiti element a s multiplikativnim inverzom elementa b u skupu $\mathbb{Z}_m$. Ako multiplikativni inverz broja b ne postoji, tada ni dijeljenje brojem b nije definirano.

Primjer 3.2. *U skupu $\mathbb{Z}_{32}$ izračunajmo $\frac{11}{9}$ i $\frac{25}{12}$.*

Rješenje. Kako je $\text{nzd}(9, 32) = 1$, to broj 9 ima multiplikativni inverz modulo 32 i taj inverz je jednak 25, jer $9 \cdot 25 = 225 \equiv 1 \pmod{32}$. Sada je

$$\frac{11}{9} = 11 \cdot 9^{-1} \bmod 32 = 11 \cdot 25 \bmod 32 = 275 \bmod 32 = 19.$$

Međutim, kako je $\text{nzd}(12, 32) = 4 \neq 1$, to broj 12 nema multiplikativni inverz modulo 32 pa dijeljenje $\frac{25}{12}$ nije definirano u skupu $\mathbb{Z}_{32}$. ◀

4 Modularno potenciranje

Cilj nam je izračunati $y = x^n \bmod m$. Kako je modularno potenciranje specijalni slučaj potenciranja u Abelovoj grupi ([3, str. 52]), to uzimajući u obzir da je trivijalna metoda računanja x^n u obliku $x \cdot x \cdot \ldots \cdot x$ vrlo neefikasna, zaključujemo i da je analogna metoda računanja $y = x^n \bmod m$ također neefikasna. Međutim, za modularno potenciranje može se iskoristiti (modificirana u modularnom smislu) jedna vrlo efikasna metoda koja koristi binarni zapis eksponenta n. Metoda je poznata pod nazivom **binarna metoda** (u literaturi se koriste i nazivi: **metoda uzastopnog kvadriranja**, **kvadriraj i množi**, **binarne ljestve**).

Želimo izračunati $y = x^n \bmod m$. Kada bismo x množili samim sobom n puta i nakon toga našli ostatak pri dijeljenju dobivenog broja s m, došli bismo do velikih brojeva i ta metoda ne bi bila efikasna.

Neka je $n = (n_k n_{k-1} \ldots n_1 n_0)_2$ binarni zapis eksponenta n. Tada je

$$n = n_k \cdot 2^k + \cdots + n_2 \cdot 2^2 + n_1 \cdot 2 + n_0,$$

gdje je $n_j \in \{0,1\},\ j = 0,1,\ldots,k$.

Sada imamo da je

$$x^n = x^{n_k \cdot 2^k + \cdots + n_2 \cdot 2^2 + n_1 \cdot 2 + n_0},$$

tj.

$$x^n = \left(x^{2^k}\right)^{n_k} \cdot \ldots \cdot \left(x^{2^2}\right)^{n_2} \cdot \left(x^2\right)^{n_1} \cdot x^{n_0}.$$

Ako npr. želimo izračunati x^{77}, kako je binarni zapis $77 = (1\,0\,0\,1\,1\,0\,1)_2$, to možemo napraviti na dva načina.

Čitajući binarni zapis broja 77 s desna na lijevo, imamo da je

$$x^{77} = x \cdot (x^2)^2 \cdot ((x^2)^2)^2 \cdot (((((x^2)^2)^2)^2)^2)^2,$$

a čitajući ga s lijeva na desno, imamo da je

$$x^{77} = x \cdot ((x \cdot (x \cdot ((x^2)^2)^2)^2)^2)^2.$$

Na osnovu prethodnog vidimo da je moguće napisati dva algoritma za modularno potenciranje, tj. za računanje $y = x^n \bmod m$, gdje je binarni zapis eksponenta $n = (n_k n_{k-1} \ldots n_1 n_0)_2$.

Algoritam 1 (Binarna metoda slijeva na desno)

$y = 1$
za $i = k, \ldots, 1, 0$ **radi**
  $y = y^2 \bmod m$
  ako $n_i = 1$ **onda** $y = x \cdot y \bmod m$

Algoritam 2 (Binarna metoda zdesna na lijevo)

$y = 1, \quad z = x$
za $i = 0, 1, \ldots, k-1$ **radi**
  ako $n_i = 1$ **onda** $y = y \cdot z \bmod m$
  $z = z^2 \bmod m$
$y = y \cdot z \bmod m$

Oba navedena algoritma imaju isti broj operacija kvadriranja i množenja. Prednost algoritma binarne metode slijeva na desno je u tome što se prilikom množenja uvijek množi s istim brojem x ($y = x \cdot y$). Kako je često, naročito u kriptografiji, taj x malen (čak jednak 2), to je u tom slučaju ova operacija vrlo brza (jeftina). Ta prednost se povećava povećanjem broja jedinica u binarnom zapisu od n.

Primjer 4.1. *Izračunajmo* $y = 567^{321} \bmod 793$.

Rješenje. Za računanje ćemo koristiti algoritam binarne metode slijeva na desno.

Imamo binarni zapis $321 = (101000001)_2$. Prolaz kroz algoritam može se prikazati tablicom:

i	$y = y^2 \bmod 793$	n_i	$y = y \cdot 567 \bmod 793$
	1		
8	$1^2 \bmod 793 = 1$	1	$1 \cdot 567 \bmod 793 = 567$
7	$567^2 \bmod 793 = 324$	0	
6	$324^2 \bmod 793 = 300$	1	$300 \cdot 567 \bmod 793 = 398$
5	$398^2 \bmod 793 = 597$	0	
4	$597^2 \bmod 793 = 352$	0	
3	$352^2 \bmod 793 = 196$	0	
2	$196^2 \bmod 793 = 352$	0	
1	$352^2 \bmod 793 = 196$	0	
0	$196^2 \bmod 793 = 352$	1	$352 \cdot 567 \bmod 793 = 541$

.

Dakle, $y = 567^{321} \bmod 793 = 541$.

Ako bismo isti račun proveli korištenjem algoritma binarne metode zdesna na lijevo, dobili bismo tablicu:

i	n_i	$y = y \cdot z \bmod 793$	$z = z^2 \bmod 793$
		1	567
0	1	$1 \cdot 567 \bmod 793 = 567$	$567^2 \bmod 793 = 324$
1	0		$324^2 \bmod 793 = 300$
2	0		$300^2 \bmod 793 = 391$
3	0		$391^2 \bmod 793 = 625$
4	0		$625^2 \bmod 793 = 469$
5	0		$469^2 \bmod 793 = 300$
6	1	$567 \cdot 300 \bmod 793 = 398$	$300^2 \bmod 793 = 391$
7	0		$391^2 \bmod 793 = 625$
		$398 \cdot 625 \bmod 793 = 541$	

.

Dakle, $y = 567^{321} \bmod 793 = 541$. ◀

Pogledajmo sada jedno poboljšanje algoritma binarne metode slijeva na desno. Poboljšanje se sastoji u promatranju grupa od t znamenki (tzv. prozora) u binarnom zapisu broja n, tj. promatra se prikaz eksponenta n u sustavu s bazom $b = 2^t$, $t \geq 1$. Primjerice, ako je baza 4 (gledamo grupe

od po dvije znamenke) i želimo računati x^{77}, najprije ćemo izračunati x, x^2 i x^3 te kako je $77 = (1\,00\,11\,01)_2 = (1\,0\,3\,1)_4$, imamo

$$x^{77} = x \cdot ((x^4)^4 \cdot x^3)^4.$$

Općenito, neka je $n = (n_k \dots n_1 n_0)_b$ prikaz eksponenta n u sustavu s bazom $b = 2^t$, za neki $t \geq 1$. Tada imamo sljedeći algoritam.

Algoritam 3

$x_0 = 1$
za $i = 1, 2, \dots, 2^t - 1$ **radi**
  $x_i = x_{i-1} \cdot x \bmod m$
$y = 1$
za $i = k, \dots, 1, 0$ **radi**
  $y = y^b \bmod m$
  $y = y \cdot x_{n_i} \bmod m$

Primjer 4.2. *Izračunajmo* $y = 123^{10763} \bmod 45678$.

Rješenje. Imamo da je $10763 = (25013)_8$ zapis broja 10763 u sustavu s bazom $8 = 2^3$. Prolaz kroz algoritam može se prikazati pomoću sljedeće dvije tablice:

i	$x_i = x_{i-1} \cdot 123 \bmod 45678$
0	$x_0 = 1$
1	$x_1 = 1 \cdot 123 \bmod 45678 = 123$
2	$x_2 = 123 \cdot 123 \bmod 45678 = 15129$
3	$x_3 = 15129 \cdot 123 \bmod 45678 = 33747$
4	$x_4 = 33747 \cdot 123 \bmod 45678 = 39861$
5	$x_5 = 39861 \cdot 123 \bmod 45678 = 15357$
6	$x_6 = 15357 \cdot 123 \bmod 45678 = 16113$
7	$x_7 = 16113 \cdot 123 \bmod 45678 = 17745$

,

i	$y = y^8 \bmod 45678$	n_i	$y = y \cdot x_{n_i} \bmod 45678$
	1		
4	$1^8 \bmod 45678 = 1$	2	$1 \cdot 15129 \bmod 45678 = 15129$
3	$15129^8 \bmod 45678 = 26259$	5	$26259 \cdot 15357 \bmod 45678 = 14079$
2	$14079^8 \bmod 45678 = 33747$	0	$33747 \cdot 1 \bmod 45678 = 33747$
1	$33747^8 \bmod 45678 = 27135$	1	$27135 \cdot 123 \bmod 45678 = 3111$
0	$3111^8 \bmod 45678 = 35967$	3	$35967 \cdot 33747 \bmod 45678 = 22533$

.

Dakle, $y = 123^{10763} \bmod 45678 = 22533$. ◀

Smanjenjem broja predračunanja vrijednosti x_j, Algoritam 3 moguće je poboljšati tako da za svaki $0 \leq i \leq k$, ako je $n_i \neq 0$, pišemo $n_i = 2^{h_i} \cdot u_i$, gdje je u_i neparan, a ako je $n_i = 0$, onda je $h_i = u_i = 0$.

Algoritam 4

$x_0 = 1, \quad x_1 = x \bmod m, \quad x_2 = x^2 \bmod m$
za $i = 1, 2, \ldots, 2^{t-1} - 1$ **radi**
  $x_{2i+1} = x_{2i-1} \cdot x_2 \bmod m$
$y = 1$
za $i = k, \ldots, 1, 0$ **radi**
  $y = \left(y^{2^{t-h_i}} \cdot x_{u_i}\right)^{2^{h_i}} \bmod m$

Primjer 4.3. *Izračunajmo sada* $y = 123^{10763} \bmod 45678$ *primjenom Algoritma 4.*

Rješenje. Znamo da je $10763 = (25013)_8$ pa prolaz kroz algoritam možemo prikazati pomoću sljedeće dvije tablice:

	$x_0 = 1$
	$x_1 = 123$
	$x_2 = 123^2 \bmod 45678 = 15129$

i	$x_{2i+1} = x_{2i-1} \cdot x_2 \bmod 45678$
1	$x_3 = 123 \cdot 15129 \bmod 45678 = 33747$
2	$x_5 = 33747 \cdot 15129 \bmod 45678 = 15357$
3	$x_7 = 15357 \cdot 15129 \bmod 45678 = 17745$

,

i	n_i	h_i	u_i	$y \to \left(y^{2^{t-h_i}} \cdot x_{u_i}\right)^{2^{h_i}} \bmod m$
				1
4	2	1	1	$\left(1^4 \cdot 123\right)^2 \bmod 45678 = 15129$
3	5	0	5	$\left(15129^8 \cdot 15357\right)^1 \bmod 45678 = 14079$
2	0	0	0	$\left(14079^8 \cdot 1\right)^1 \bmod 45678 = 33747$
1	1	0	1	$\left(33747^8 \cdot 123\right)^1 \bmod 45678 = 3111$
0	3	0	3	$\left(3111^8 \cdot 33747\right)^1 \bmod 45678 = 22533$

.

Dakle, $y = 123^{10763} \bmod 45678 = 22533$. ◀

Pogledajmo broj množenja i kvadriranja u prethodnim algoritmima, uz napomenu da se množenja s 1 i kvadriranje 1^2 ne broje. Neka je $k+1$ broj bitova u zapisu eksponenta n i $wk(n)$ broj jedinica u tom zapisu. Tada u algoritmima 1 i 2 imamo $k+1$ kvadriranja i $wk(n)-1$ množenja. Za slučajan eksponent $0 \leq n < m$ očekujemo oko $\lfloor \ln m \rfloor$ kvadriranja i $0,5 \cdot (\lfloor \ln m \rfloor + 1)$ množenja. Ako uzmemo da kvadriranje aproksimativno "košta" koliko i množenje, onda je za očekivati $1,5 \cdot \lfloor \ln m \rfloor$ množenja.

Neka je $r+1$ broj t–bitnih riječi u n. Tada je

$$r = \left\lceil \frac{k+1}{t} \right\rceil - 1 = \left\lfloor \frac{k}{t} \right\rfloor,$$

gdje $\lceil x \rceil$ predstavlja funkciju **najmanje cijelo**, koja realnom broju x pridružuje najmanji cijeli broj koji je veći ili jednak x.

Sada imamo da je broj kvadriranja u Algoritmu 3 jednak rt, pa je

$$rt = \left\lfloor \frac{k}{t} \right\rfloor \cdot t = k - (k \bmod t).$$

Dobili smo da je

$$k - (t-1) \leq rt \leq k,$$

iz čega zaključujemo da Algoritam 3 može smanjiti broj kvadriranja za $t-1$ u odnosu na algoritme 1 i 2. Optimalna vrijednost za t u Algoritmu 3 ovisi od vrijednosti k.

Broj kvadriranja u Algoritmu 4 jednak je $rt + h_r$, gdje je $0 \leq h_r \leq k \bmod t$. Sada imamo da je

$$k - (t-1) \leq rt \leq rt + h_r \leq rt + (k \bmod t) = k$$

odnosno

$$k - (t-1) \leq rt + h_r \leq k,$$

pa vidimo da je granica za broj kvadriranja u Algoritmu 4 ista kako kod Algoritma 3.

Dobivene rezultate možemo predstaviti sljedećom tablicom:

Alg	Predračunanja		Kvadriranja	Množenja	
	Kv	Mn		Najgori slučaj	Prosječan slučaj
1	0	0	$k+1$	k	$k/2$
2	0	0	$k+1$	k	$k/2$
3	1	2^t-3	$k-(t-1) \leq rt \leq k$	$r-1$	$r(2^t-1)/2^t$
4	1	$2^{t-1}-1$	$k-(t-1) \leq rt+h_r \leq k$	$r-1$	$r(2^t-1)/2^t$

Sljedeći algoritam, poznat pod nazivom **klizni prozor** (engl. sliding–window), predstavlja još jedno poboljšanje Algoritma 3. Poboljšanje se ogleda, kao i kod Algoritma 4, u smanjenju broja predračunanja vrijednosti x_j, ali u ovom slučaju također, smanjenjem prosječnog broja operacija množenja. Napomenimo da se prirodni broj t, koji se bira proizvoljno i učitava kao ulazni podatak, naziva **veličina prozora**.

Algoritam 5

$x_1 = x \bmod m, \quad x_2 = x^2 \bmod m$
za $i = 1, 2, \ldots, 2^{t-1} - 1$ **radi**

$x_{2i+1} = x_{2i-1} \cdot x_2 \bmod m$
$y = 1$
$i = k$
dok je $i \geq 0$ **radi**

ako $n_i = 0$

onda

$y = y^2 \bmod m$

$i = i - 1$

inače

nađi najveći niz bitova $n_i n_{i-1} \ldots n_r$ **takav**

da je $i - r + 1 \leq t$ **i** $n_r = 1$

$y = y^{2^{i-r+1}} \cdot x_{(n_i n_{i-1} \ldots n_r)_2} \bmod m$

$i = r - 1$

Primjer 4.4. *Izračunajmo opet* $y = 123^{10763} \bmod 45678$.

Rješenje. Vrijedi $10763 = (10101000001011)_2$ pa odaberimo $t = 3$. Vrijednosti x_1, x_2, x_3, x_5 i x_7 su iste kao u Primjeru 4.3. Prolaz kroz algoritam se može prikazati pomoću sljedeće tablice:

i	n_i	$n_i \dots n_r$	r	y
				1
13	1	$(101)_2 = 5$	11	$1^8 \cdot 15357 \bmod 45678 = 15357$
10	0			$15357^2 \bmod 45678 = 1935$
9	1	$(1)_2 = 1$	9	$1935^2 \cdot 123 \bmod 45678 = 14079$
8	0			$14079^2 \bmod 45678 = 21399$
7	0			$21399^2 \bmod 45678 = 40929$
6	0			$40929^2 \bmod 45678 = 33747$
5	0			$33747^2 \bmod 45678 = 16113$
4	0			$16113^2 \bmod 45678 = 40695$
3	1	$(101)_2 = 5$	1	$40695^8 \cdot 15357 \bmod 45678 = 35829$
0	1	$(1)_2 = 1$	0	$35829^2 \cdot 123 \bmod 45678 = 22533$

Dakle, $y = 123^{10763} \bmod 45678 = 22533$. ◀

5 Montgomeryjeva redukcija

Još jedna metoda, koja predstavlja poboljšanje direktne metode za računanje broja $x \cdot_m y$, gdje nakon izračunatog broja xy treba naći ostatak pri dijeljenju s modulom m, je Montgomeryjeva redukcija [7]. Ideja je izbjegavanje klasične modularne redukcije, tj. dijeljenja.

Neka su m i R prirodni brojevi takvi da je $m < R$ i $\text{nzd}(m, R) = 1$ te neka je x cijeli broj takav da je $0 \leq x < mR$. Izraz $xR^{-1} \bmod m$ naziva se **Montgomeryjeva redukcija** od x modulo m u odnosu na R, a izraz $xR \bmod m$ naziva se **Montgomeryjev prikaz** od x. Ako je m zapisan u bazi b i u tom prikazu ima n znamenki, onda se za R obično uzima b^n. Sljedeća propozicija (za dokaz vidjeti [2, 6]) pokazuje da se $xR^{-1} \bmod m$ može izračunati bez klasičnog dijeljenja, tj. da se dijeljenje s m zamjenjuje dijeljenjem s R, što, u slučaju kada je $R = b^n$, predstavlja jednostavni pomak za n znamenki. Očigledno je uvjet $R > m$ zadovoljen, dok će uvjet $\text{nzd}(m, R) = 1$ biti ispunjen ako i samo ako je $\text{nzd}(m, b) = 1$.

Propozicija 5.1. *Neka su $m < R$ prirodni brojevi takvi da je $\text{nzd}(m, R) = 1$ i neka je x cijeli broj takav da je $0 \leq x < mR$. Neka je $m' = -m^{-1} \bmod R$ i $U = xm' \bmod R$. Tada je $V = (x + Um)/R$ cijeli broj i vrijedi $V \equiv xR^{-1} \pmod m$. Nadalje vrijedi da je $xR^{-1} \bmod m = V$ ili je $xR^{-1} \bmod m = V - m$.*

Neka je m prirodni broj, koji u bazi b ima zapis $m = (m_{n-1} \dots m_1 m_0)_b$, gdje je $\text{nzd}(m, b) = 1$. Neka je $R = b^n$, $m' = -m^{-1} \bmod b$. Sljedeći algoritam računa Montgomeryjevu redukciju $y = xR^{-1} \bmod m$ zadanog broja

$x < mR$, koji u bazi b ima zapis $x = (x_{2n-1} \dots x_1 x_0)_b$. Napomenimo da se, zbog izbora $R = b^n$, u algoritmu, za razliku od Propozicije 5.1, prilikom računanja m' i U umjesto modulo R računa modulo b. Vrijednost $m' = -m^{-1} \bmod b$ se vrlo jednostavno može izračunati pomoću proširenog Euklidovog algoritma ([6, Algoritam 2.107]).

Algoritam 6 (Montgomeryjeva redukcija)

$y = x \qquad (y = (y_{2n-1} \dots y_1 y_0)_b)$
za $i = 0, 1, \dots, n-1$ **radi**
  $u_i = y_i m' \bmod b$
  $y = y + u_i m b^i$
$y = y/b^n$
ako $y \geq m$ **onda** $y = y - m$

Primjer 5.1. *Izračunajmo Montgomeryjevu redukciju* $xR^{-1} \bmod m$*, gdje je* $x = 8363481$*,* $m = 63457$ *i* $R = 10^5$.

Rješenje. Kako je $b = 10$, $\text{nzd}(63457, 10) = 1$ i $x = 8363481 < 63457 \cdot 10^5$, to su zadovoljeni svi potrebni uvjeti. Imamo da je

$$m' = -63457^{-1} \bmod 10 = -3 \bmod 10 = 7$$

pa prolaz kroz petlju algoritma možemo prikazati sljedećom tablicom:

i	$u_i = y_i \cdot m' \bmod b$	$y = y + u_i \cdot m \cdot b^i$
		$836348\underline{1}$
0	$1 \cdot 7 \bmod 10 = 7$	$8363481 + 7 \cdot 63457 \cdot 10^0 = 880768\underline{0}$
1	$8 \cdot 7 \bmod 10 = 6$	$8807680 + 6 \cdot 63457 \cdot 10^1 = 1261\underline{5}100$
2	$1 \cdot 7 \bmod 10 = 7$	$12615100 + 7 \cdot 63457 \cdot 10^2 = 570\underline{3}5000$
3	$5 \cdot 7 \bmod 10 = 5$	$57035000 + 5 \cdot 63457 \cdot 10^3 = 37\underline{4}320000$
4	$2 \cdot 7 \bmod 10 = 4$	$374320000 + 4 \cdot 63457 \cdot 10^4 = 2912600000$

Sada je

$$y = 2912600000/10^5 = 29126$$

pa kako je $y < m$ to zaključujemo da je tražena Montgomeryjeva redukcija jednaka

$$xR^{-1} \bmod m = 29126.$$

◀

Broj $\text{Mont}(x,y) = xyR^{-1} \bmod m$, koji se naziva **Montgomeryjev produkt** brojeva x i y, možemo izračunati koristeći ideju Montgomeryjeve redukcije. Ovako definiran produkt je dobro definiran, jer je $xy < m^2 < mR$.

Kako je

$$\text{Mont}(xR \bmod m, yR \bmod m) = (xR)(yR)R^{-1} = xyR \bmod m,$$

to vidimo da se za brojeve u Montgomeryjevom prikazu modularno množenje može provesti bez modularne redukcije modulo m.

Neka je $m = (m_{n-1} \dots m_1 m_0)_b$ prirodni broj te neka je $R = b^n$, pri čemu je $\text{nzd}(m,b) = 1$. Neka je $m' = -m^{-1} \bmod b$. Sljedeći algoritam, koristeći ideju Montgomeryjeve redukcije, računa Montgomeryjev produkt

$$z = \text{Mont}(x,y) = xyR^{-1} \bmod m$$

cijelih brojeva $x = (x_{n-1} \dots x_1 x_0)_b$ i $y = (y_{n-1} \dots, y_1 y_0)_b$, takvih da je $0 \leq x, y < m$.

Algoritam 7 (Montgomeryjev produkt)

$z = 0 \qquad (z = (z_n \dots z_1 z_0)_b)$
za $i = 0, 1, \dots, n-1$ **radi**
  $u_i = (z_0 + x_i y_0) m' \bmod b$
  $z = (z + x_i y + u_i m)/b$
ako $z \geq m$ **onda** $z = z - m$

Primjer 5.2. *Izračunajmo Montgomeryjev produkt* $\text{Mont}(x,y)$ *brojeva* $x = 4563$ *i* $y = 2274$ *modulo* $m = 83617$.

Rješenje. Kako modul m ima 5 znamenki, to je $n = 5$. Kako je baza $b = 10$, uzet ćemo $R = 10^5$. Očigledno je $0 \leq x, y < 83617$ i $\text{nzd}(83617, 10) = 1$ pa su zadovoljeni potrebni uvjeti i možemo primijeniti Algoritam 7. Imamo da je

$$m' = -m^{-1} \bmod 10 = -83617^{-1} \bmod 10 = -3 \bmod 10 = 7$$

pa, kao i u prethodnom primjeru, prolaz kroz petlju algoritma možemo prikazati sljedećom tablicom:

i	$u_i = (z_0 + x_i y_0) m' \bmod b$	$z = (z + x_i y + u_i m)/b$
		$\underline{\mathbf{0}}$
0	$(0 + 3 \cdot 4) \cdot 7 \bmod 10 = 4$	$(0 + 3 \cdot 2274 + 4 \cdot 83617)/10 = 3412\underline{\mathbf{9}}$
1	$(9 + 6 \cdot 4) \cdot 7 \bmod 10 = 1$	$(34129 + 6 \cdot 2274 + 1 \cdot 83617)/10 = 1313\underline{\mathbf{9}}$
2	$(9 + 5 \cdot 4) \cdot 7 \bmod 10 = 3$	$(13139 + 5 \cdot 2274 + 3 \cdot 83617)/10 = 2753\underline{\mathbf{6}}$
3	$(6 + 4 \cdot 4) \cdot 7 \bmod 10 = 4$	$(27536 + 4 \cdot 2274 + 4 \cdot 83617)/10 = 3711\underline{\mathbf{0}}$
4	$(0 + 0 \cdot 4) \cdot 7 \bmod 10 = 0$	$(37110 + 0 \cdot 2274 + 0 \cdot 83617)/10 = 3711$

Sada je

$$z = 3711$$

pa kako je $z < m$ to zaključujemo da je traženi Montgomeryjev produkt jednak

$$\text{Mont}(4563, 2274) = 3711.$$

◀

Vidjeli smo da se za brojeve u Montgomeryjevom prikazu modularno množenje može provesti bez modularne redukcije modulo m. Jasno je da modularnu redukciju trebamo da bismo uopće dobili Montgomeryjev prikaz brojeva. Međutim, ako više puta koristimo jedan te isti broj, kao što je slučaj kod potenciranja, tada je Montgomeryjeva redukcija znatno efikasnija od obične modularne redukcije. Ranije navedene metode potenciranja, koje se odnose na potenciranje u bilo kojoj Abelovoj grupi, možemo poboljšati korištenjem Montgomeryjeve redukcije. Tako kombinirajući Algoritam 7 s Algoritmom 1 dobivamo algoritam za **Montgomeryjevo potenciranje** kojim se računa $x^n \bmod m$.

Neka su $m = (m_{k-1} \dots m_1 m_0)_b$ i $x < m$ prirodni brojevi te neka je $R = b^k$, $m' = -m^{-1} \bmod b$, $n = (n_t \dots n_1 n_0)_2$, $n_t = 1$. Montgomeryjev algoritam za računanje $y = x^n \bmod m$ ima sljedeći oblik:

Algoritam 8

$z = \text{Mont}(x, R^2 \bmod m)$
$y = R \bmod m$
za $i = t, \dots, 1, 0$ **radi**
  $y = \text{Mont}(y, y)$
  ako $n_i = 1$ **onda** $y = \text{Mont}(y, z)$
$y = \text{Mont}(y, 1)$

Zaista, kako je

$$z = \text{Mont}(x, R^2 \bmod m) = xR^2R^{-1} \bmod m = xR \bmod M,$$

to se u petlji izračuna $x^n R \bmod m$, i na kraju

$$y = \text{Mont}(y, 1) = \text{Mont}(x^n R \bmod m, 1) = x^n R R^{-1} \bmod m = x^n \bmod m.$$

Primjer 5.3. *Primjenom Algoritma 8 izračunajmo* $y = 3571^{1171} \bmod 72639$.

Rješenje. Imamo binarni zapis $1171 = (10010010011)_2$. Kako je $m = 72639$ to je $k = 5$ pa stavimo $R = 10^5$. Sada je

$$R \bmod m = 27361, \quad R^2 \bmod m = 6787 \quad \text{i} \quad z = \text{Mont}(x, R^2 \bmod m) = 6676.$$

Prolaz kroz petlju algoritma prikažimo tablicom:

i	$y = \text{Mont}(y, y)$	n_i	$y = \text{Mont}(y, z)$
10	$\text{Mont}(27361, 27361) = 27361$	1	$\text{Mont}(27361, 6676) = 6676$
9	$\text{Mont}(6676, 6676) = 14404$	0	
8	$\text{Mont}(14404, 14404) = 47878$	0	
7	$\text{Mont}(47878, 47878) = 65812$	1	$\text{Mont}(65812, 6676) = 27487$
6	$\text{Mont}(27487, 27487) = 43678$	0	
5	$\text{Mont}(43678, 43678) = 1531$	0	
4	$\text{Mont}(1531, 1531) = 460$	1	$\text{Mont}(460, 6676) = 44602$
3	$\text{Mont}(44602, 44602) = 48487$	0	
2	$\text{Mont}(48487, 48487) = 69802$	0	
1	$\text{Mont}(69802, 69802) = 57559$	1	$\text{Mont}(57559, 6676) = 47458$
0	$\text{Mont}(47458, 47458) = 43678$	1	$\text{Mont}(43678, 6676) = 18205$

Dakle

$$3571^{1171} \bmod 72639 = \text{Mont}(18205, 1) = 12643.$$

◀

Literatura

[1] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[2] A. Dujella, *Algoritmi u teoriji brojeva*, Skripta, PMF, Zagreb, 2021.

[3] K. Horvatić, *Linearna algebra*, Golden marketing – Tehnička knjiga, Zagreb, 2004.

[4] B. Ibrahimpašić, S. Ibrahimpašić, *Linearne kongruencije i sistemi linearnih kongruencija*, MAT–KOL, Vol XX (1)(2014), 27–36.

[5] B. Ibrahimpašić, *Kongruencije oblika* $x^n \equiv 0 \pmod{m}$, Osječki matematički list, **15** (1) (2015), 33–40.

[6] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Bora Raton, 1996.

[7] P. L. Montgomery, *Modular Multiplication Without Trial Division*, Math. Comp. **44** (1985), 519–521.