*Hello, World!*

# Алгоритми теорије бројева - Део 2

***Марко Савић***

У претходном броју смо приказали ефикасне алгоритме за утврђивање да ли је број прост, налажење свих простих бројева до неког датог броја и налажење највећег заједничког делиоца за два природна броја. У овом броју ћемо писати о још неколико основних алгоритама теорије бројева.

## Проширени Еуклидов алгоритам

Познато је да за природне бројеве $a$ и $b$ постоје цели бројеви $x$ и $y$ такви да важи $nzd(a,b) = ax + by$. Да бисмо те бројеве добили, проширићемо Еуклидов алгоритам за налажење највећег заједничког делиоца, који је описан у прошлом броју. Овакав проширени алгоритам за задате природне бројеве поред највећег заједничког делиоца враћа тражене бројеве $x$ и $y$.

**Алгоритам EuklidProširen**
**Улаз:** Природни бројеви $a$ и $b$.
**Излаз:** $(nzd(a,b),\ x,\ y)$.

```
if b = 0
        return (a, 1, 0)
else
        (d, x, y) ←EuklidProširen(b, amodb)
        return (d, y, x − ⌊a/b⌋y)
```

Попут Еуклидовог алгоритма, сложеност проширеног Еуклидовог алгоритма је $O(\log b)$. Индукцијом по броју рекурзивних позива се лако може показати да смо овим поступком добили управо бројеве које смо тражили. Детаљан доказ остављамо читаоцу за вежбу.

## Брзо степеновање

Често је у алгоритмима потребно израчунати степен неког броја где је експонент природан број. Како $a^b$ има изузетно велику вредност већ за релативно мале вредности $a$ и $b$, са резултујућим бројем углавном није могуће ефикасно радити. Срећом, у теорији бројева нам најчешће не треба

конкретна вредност тог степеновања, већ само $a^b \pmod M$, односно остатак који $a^b$ даје при дељењу са $M$.

Тривијалан метод да се $a^b \pmod M$ израчуна састојао би се од $b$ множења, при чему након сваког множења чувамо само остатак при дељењу са $M$. Овај поступак има временску сложеност $O(b)$. Међутим, често је број $b$ веома велик, те тада овај метод није довољно ефикасан.

Да бисмо убрзали поступак рачунања степена, приметимо да важи следеће.

$$a^b = (a^{b/2})^2, \text{ ако је } b \text{ парно,}$$

$$a^b = a(a^{\lfloor b/2 \rfloor})^2, \text{ ако је } b \text{ непарно.}$$

На основу овога, можемо да напишемо следећи рекурзивни алгоритам:

**Алгоритам BrzoStepenovanje**
**Улаз:** Природни бројеви $a$, $b$ и $M$.
**Излаз:** $a^b (mod M)$.

```
if b = 0
        return 1
else
        t ← BrzoStepenovanje(a, ⌊b/2⌋, M)
        if b је парно
                return t^2 mod M
        else
                return at^2 mod M
```

Сложеност овог алгоритма је $O(\log b)$.

## Модуларни мултипликативни инверз

Рачунање $a \cdot b \pmod M$ је једноставно извести, али ако нам треба инверзна операција, тј. операцији множења по модулу $M$, ствари постају компликованије.

У аритметици са реалним бројевима лако је решити једначину $b \cdot x = a$, решење је $x = a/b$, али како добити решење конгруенције $b \cdot x \equiv a \pmod M$, где су $a$, $b$, $x$ и $M$ сви цели бројеви ($0 \leq a, b, x < M$)? Број $x$ за неке конгруенције овог типа не мора да постоји, а за неке друге не мора да буде јединствен. Међутим, познато је да $x$ постоји и једнозначно је одређен ако и само ако су $b$ и $M$ узајамно прости.

Ако са $b^{-1}$ означимо решење конгруенције $b \cdot x \equiv 1 \pmod M$, онда се решење једначине $b \cdot x \equiv a \pmod M$ добија тако што обе стране помно-

жимо са $b^{-1}$, па добијамо $x \equiv a \cdot b^{-1} \pmod{M}$. Број $b^{-1}$ се назива модуларни мултипликативни инверз броја $b$. Циљ нам је да израчунамо $b^{-1}$ за дате $b$ и $M$.

Тривијалан начин за добијање модуларног мултипликативног инверза је да пробамо све могуће вредности за $b^{-1}$ и видимо која од тих вредности задовољава тражену конгруенцију. То је алгоритам временске сложености $O(M)$.

## Инверз коришћењем мале Фермаове теореме

Уколико је $M$ прост број, можемо конструисати знатно бржи алгоритам. У помоћ нам прискаче мала Фермаова теорема, на основу које знамо да је $b^{M-1} \equiv 1 \pmod{M}$. Помножимо обе стране са $b^{-1}$ и добићемо $b^{M-2} \equiv b^{-1} \pmod{M}$. Дакле, све што нам треба да бисмо добили модуларни мултипликативни инверз је да израчунамо $b^{M-2}$ по модулу $M$. А то можемо ефикасно урадити коришћењем описаног алгоритма за брзо степеновање, са једином изменом што ћемо сва множења у том алгоритму радити по модулу $M$. Стога је временска сложеност овог поступка је $O(\log M)$.

## Инверз коришћењем проширеног Еуклидовог алгоритма

Ако претпоставимо да су $b$ и $M$ узајамно прости, онда постоје бројеви $x$ и $y$ за које важи $bx + My = 1$. Ову једнакост можемо написати као конгруенцију по модулу $M$, па добијамо $bx + My \equiv 1 \pmod{M}$, односно $x \equiv b^{-1} \pmod{M}$. Ово значи да ћемо применом проширеног Еуклидовог алгоритма на бројеве $b$ и $M$ добити $x$ које представља мултипликативни инверз броја $b$ по модулу $M$. Временска сложеност овог поступка је једнака временској сложености проширеног Еуклидовог алгоритма. А то је $O(\log M)$.

## Сви модуларни мултипликативни инверзи

Понекад нам је потребно да израчунамо мултипликативне инверзе за све бројеве $b \in \{1,2, \dots M-1\}$. Користећи претходни поступак јасно је да то можемо урадити рачунањем сваког инверза понаособ, што би нам укупно узело $O(M \log M)$ времена. Међутим, можемо боље!

Претпоставимо да смо већ израчунали све инверзе за бројеве $1,2, \dots, n-1$ и да сада желимо да израчунамо инверз за $n$. Нека је $k = \lfloor M/n \rfloor$ и $r = M \bmod n$ (остатак при дељењу са $n$). Дакле, $M = kn + r$, $r < n$ и $kn + r \equiv 0 \pmod{M}$. Пошто је, према претпоставци, $r < n$, $r^{-1}$ је већ израчунато, те можемо обе стране претходне конгруенције да помножимо

са њиме. Добијамо $kr^{-1}n + 1 \equiv 0 \pmod{M}$, тј. $1 \equiv -kr^{-1}n \pmod{M}$, из чега видимо да је $-kr^{-1}$ модуларни инверз броја $x$.

**Алгоритам SviModularniInverzi**
**Улаз:** Природан број $M$.
**Излаз:** Низ који садржи све модуларне инверзе по модулу $M$.

```
inverzi[1] ← 1
for n ← 2 ... M − 1
        k ← ⌊M/n⌋
        r ← M mod n
        inverzi[n] ← ((M − k) · inverzi[r]) mod M
return inverzi
```

Овај алгоритам је временске сложености $O(M)$, што је за $\log M$ фактор боље од алгоритма који рачуна сваки инверз независно од других. Приметимо да је ово оптималан алгоритам, јер није могуће брже попунити низ са $M$ бројева.

## Кинеска теорема о остацима

Чувена кинеска теорема о остацима каже да ако су $M_1, M_2, \ldots, M_n$ по паровима узајамно прости природни бројеви, тада систем конгруенција

$$\begin{aligned} x &\equiv r_1 \pmod{M_1} \\ x &\equiv r_2 \pmod{M_2} \\ &\cdots \\ x &\equiv r_n \pmod{M_n} \end{aligned}$$

има јединствено решење по модулу $P = M_1 \cdot M_2 \cdot \ldots \cdot M_n$.

Нас занима како да ефикасно израчунамо број $x$ који представља то решење. Нека је $P_i = M/M_i$. Ако је $P_i^{-1}$ мултипликативни инверз од $P_i$ по модулу $M_i$, тј. $P_i^{-1}P \equiv 1 \pmod{M_i}$, лако се може проверити да је

$$x \equiv r_1P_1P_1^{-1} + r_2P_2P_2^{-1} + \cdots + r_nP_nP_n^{-1} \pmod{P}$$

решење задатог система.

Све што треба да урадимо да бисмо ово решење израчунали је да израчунамо модуларне мултипликативне инверзе за свако $P_i$. Због тога је временска сложеност овог израчунавања

$$O(\log M_1 + \log M_2 + \cdots + \log M_n) = O(\log P).$$

## Задаци

**1.** Доказати исправност проширсног Еуклидовог алгоритма.

**2.** Ако су $a$ и $b$ природни бројеви такви да је $a$ дељиво са $b$, доказати да је $a/b \equiv a \cdot b^{-1} \pmod{M}$, где је $b^{-1}$ мултипликативни инверз броја $b$ по модулу $M$.

**3.** Написати програм који за дате природне бројеве $n$, $b$ и $M$ што брже израчунава суму $(1 + b + b^2 + b^3 + \cdots + b^n) \pmod{M}$. (Напомсна: $M$ није обавезно прост број.)

**4.** Написати програм који за дати природан број $n$ и прост број $p$ израчунава суму свих делиоца броја $n$ по модулу $p$.

**5.** За дате природне бројеве $n$ и $k$ $(k \leq n \leq 10^{18})$ написати што ефикаснији програм који израчунава последњих 10 цифара броја $\binom{n}{k}$.

**Статијата прв пат е објавена во списанието Тангента на ДМ на Србија во 2016/17 година**