PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **29** (2001/2002)
Številka 3
Strani 168–170

Štefko Miklavič:

MODULARNA REDUKCIJA IN MERSENNOVA ŠTEVILA

Ključne besede: matematika, teorija števil, deljivost, šifriranje z javnimi ključi, RSA.

Elektronska verzija: http://www.presek.si/29/1478-Miklavic.pdf

© 2001 Društvo matematikov, fizikov in astronomov Slovenije
© 2010 DMFA – založništvo

Vse pravice pridržane. Razmnoževanje ali reproduciranje celote ali posameznih delov brez poprejšnjega dovoljenja založnika ni dovoljeno.

MODULARNA REDUKCIJA IN MERSENNOVA ŠTEVILA

Pri računanju z velikimi števili večkrat naletimo na naslednji problem:

Dani sta naravni števili a in m. Poišči ostanek pri deljenju števila a s številom m.

Drugače problem zastavimo lahko tudi takole:

Poišči tako celo število b med 0 in $m-1$, ki je kongruentno številu a po modulu m: $a \equiv b \pmod{m}$.

Ali še drugače:

Iščemo tako celo število b med 0 in $m-1$, da bo razlika $a-b$ deljiva z m.

Pravimo, da želimo število a *reducirati po modulu* m, sam postopek pa imenujemo *modularna redukcija*. Problem modularne redukcije nastopi npr. v eni izmed najbolj znanih metod za šifriranje z javnimi ključi – metodi RSA. Ker je potrebno pri uporabi metode modularno redukcijo izvršiti velikokrat, je hitrost njene izvedbe eden izmed dejavnikov, ki pomembno vplivajo na hitrost celotne metode in s tem tudi na njeno uporabnost. Več o šifriranju z javnimi ključi in metodi RSA si bralec lahko prebere v članku *M. Vencelj, Šifriranje z javnim ključem, Presek 22, št. 6 (1994-1995), str. 354–357.*

Modularno redukcijo običajno opravimo s celoštevilskim deljenjem: število a delimo s številom m in poiščemo ostanek. Toda to je v splošnem kar zamudna naloga, še posebej, če sta števili a in m veliki. Seveda si zastavimo vprašanje, ali znamo modularno redukcijo izvesti še na kakšen drugačen, hitrejši način. Če je modul m primerno izbran, je odgovor na to vprašanje pritrdilen. Pa si poglejmo, kako to storimo.

Za modul m vzemimo Mersennovo število, to je število oblike $m = 2^k - 1$, kjer je k poljubno naravno število. Zapis števila m v dvojiškem sistemu je zelo preprost – sestavljen je namreč kar iz zaporedja k enic:

$$m = \underbrace{11\cdots11}_{k}{}_{(2)}\,.$$

Zapišimo v dvojiškem sistemu tudi število a. Po potrebi bomo dvojiškemu zapisu števila a na začetku dodali nekaj ničel, tako da bo njegova dolžina $n \cdot k$ znakov (bitov) za neko naravno število n. Naj bo število A_{n-1} enako številu, ki ga v dvojiškem zapisu predstavlja prvih k bitov števila a (gledano od leve proti desni), število A_{n-2} število, ki ga predstavlja drugih k bitov števila a, in tako naprej do števila A_0, ki ga predstavlja zadnjih k bitov števila a. Število a lahko sedaj izrazimo na naslednji način:

$$a = 2^{(n-1)k} A_{n-1} + 2^{(n-2)k} A_{n-2} + \cdots + 2^{2k} A_2 + 2^k A_1 + A_0 \,,$$

kjer so $A_{n-1}, A_{n-2}, \ldots, A_1, A_0$ k-bitna števila.

Trdimo, da je število $b = A_{n-1} + A_{n-2} + \cdots + A_1 + A_0$ kongruentno številu a po modulu m. Preveriti moramo torej, da je razlika $a - b$ deljiva z m:

$$\begin{aligned} a - b &= 2^{(n-1)k} A_{n-1} + 2^{(n-2)k} A_{n-2} + \cdots + 2^k A_1 + A_0 - \\ &\quad - A_{n-1} - A_{n-2} - \cdots - A_1 - A_0 = \\ &= A_{n-1}(2^{(n-1)k} - 1) + A_{n-2}(2^{(n-2)k} - 1) + \cdots + A_1(2^k - 1) \,. \quad (1) \end{aligned}$$

Poljuben sumand vsote (1) je oblike $A_t(2^{tk} - 1)$ za neko naravno število t, $1 \le t \le n-1$ in ga zato lahko zapišemo takole:

$$\begin{aligned} A_t(2^{tk} - 1) &= A_t \cdot (2^k - 1) \cdot (2^{(t-1)k} + 2^{(t-2)k} + \cdots + 1) = \\ &= A_t \cdot m \cdot (2^{(t-1)k} + 2^{(t-2)k} + \cdots + 1) \,. \end{aligned}$$

Torej je vsak sumand vsote (1) deljiv z m in zato tudi število $a - b$. S tem je trditev dokazana.

Seveda se lahko zgodi, da je število b večje od $m - 1$. V tem primeru enak postopek ponovimo še enkrat, tokrat s številom b na mestu števila a. S ponavljanjem postopka prej ali slej pridemo do števila, ki je manjše ali enako $m - 1$ in ki pri deljenju z m da enak ostanek kot a. Modularno redukcijo smo tako izvedli s seštevanjem, ki ga lahko opravimo bistveno hitreje kot celoštevilsko deljenje.

Največkrat – npr. pri metodi RSA – naletimo na naslednjo inačico modularne redukcije: Imamo naravni števili x in y, ki sta manjši ali enaki $m - 1$. Ti dve števili zmnožimo, produkt $a = xy$ pa moramo reducirati po modulu m. V tem primeru je opisana metoda še posebej enostavna, saj je zapis števila a v dvojiškem sistemu dolg kvečjemu $2k$ bitov. Število b je zato enako vsoti dveh k-bitnih števil A_1 in A_0. Po največ dveh ponovitvah zgornjega postopka bomo dobili ustrezno število b, ki bo manjše od m.

Zaradi različnih omejitev se izkaže, da Mersennova števila za metodo RSA niso primerna. Rešitev se ponuja v tako imenovanih *posplošenih Mersennovih številih*. To so števila, ki so "podobna" Mersennovim številom, kot npr. števila oblike

- $2^n - c$, za poljubno naravno število n in fiksno naravno število c,
- $2^n - 2^m - 1$, za poljubni naravni števili $n > m$,
- $2^{4n} - 2^{3n} + 2^{2n} + 1$, za poljubno naravno število n, itd.

Pri teh številih je seveda modularna redukcija nekoliko bolj zapletena kot pri pravih Mersennovih številih, je pa zato izbira teh števil dosti večja in pestrejša.

Štefko Miklavič