ARITMETIKA DVOJIŠKIH KONČNIH OBSEGOV

JERNEJ TONEJC

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2010): 11T{06, 22, 55, 71}, 12E{05, 20, 30}, 68R05

V članku predstavimo končne obsege in aritmetiko v končnih obsegih karakteristike 2. Ti imajo pomembno vlogo v implementaciji številnih kriptosistemov in kod za odpravljanje napak. Opišemo učinkovite algoritme za računanje v polinomskih bazah končnih obsegov, ki se pogosto uporabljajo v kriptografskih aplikacijah.

ARITHMETIC OF BINARY FINITE FIELDS

We introduce finite fields and arithmetic in finite fields of characteristic 2 which play an important role in implementation of many cryptosystems and error-correcting codes. We describe efficient arithmetic algorithms in polynomial bases for finite fields which are often used in cryptographic applications.

Uvod

S končnimi obsegi so se ukvarjali ugledni matematiki, kot so Fermat, Euler, Lagrange in Legendre, ki so prispevali k razvoju teorije praštevilskih obsegov $\mathbb{Z}_p$. Splošno teorijo končnih obsegov sta začela graditi Gauss in Galois. Vendar pa se je le-ta uveljavila v uporabni matematiki šele s prihodom računalnikov, kjer ne gre brez diskretnih matematičnih struktur. Spomnimo se, da je obseg najpreprostejša algebraična struktura, v kateri lahko izvajamo vse elementarne aritmetične operacije, tj. seštevamo, odštevamo, množimo in delimo (v resnici množimo z multiplikativnim inverzom). Z razvojem teorije kodiranja, kriptografije in številnih kriptosistemov, ki uporabljajo končne obsege, se je pokazala potreba po izboljšavi algoritmov za aritmetiko nad končnimi obsegi. Pri izvajanju kriptografskih aplikacij se osnovne aritmetične operacije v obsegih izvršijo zelo velikokrat, zato je hitrost ključnega pomena. Seštevanje elementov je običajno hitro, zato pa sta množenje in še posebej računanje inverza časovno zahtevnejši operaciji.

Računalniki skoraj vedno računajo s števili, predstavljenimi v dvojiškem sistemu. Naravno število $k \in [2^n, 2^{n+1})$, kjer je $n \in \mathbb{N}$, lahko zapišemo kot

$$k = 2^n k_n + 2^{n-1} k_{n-1} + \cdots + 2k_1 + k_0\,, \quad \text{kjer je } k_i \in \mathbb{Z}_2 \ \text{ in } \ k_n \neq 0\,. \quad (1)$$