Aritmetika konačnih polja

Matijević, Martin

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:417776

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-07-03**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Martin Matijević

ARITMETIKA KONAČNIH POLJA

Diplomski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, rujan, 2022.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Pokojnoj baki Mari.

Sadržaj

Uvod

Ideja ovog rada je obraditi pitanja reprezentacije elemenata te efikasne implementacije operacija na konačnim poljima. Pokazat ćemo još neke algoritme na konačnim poljima koji su od interesa za primjene u kriptografiji.

U prvom poglavlju su dane neke osnove algebarskih struktura koje su nam potrebne. Definirane su grupe, prsteni i polja te pripadne operacije nad njima. Prisjetili smo se pojmova kongruentnosti, relacije ekvivalencije, klase ekvivalencija, integralne domene, ideala i slično. Skripta "Algebarske strukture" [6] profesora Širole je tu bila od velike pomoći te također knjiga "Introduction to Finite Fields and their Applications" [5].

U drugom poglavlju smo definirali konačno polje te dokazali razne teoreme vezane za konačna polja koristeći knjigu "Teorija brojeva" [2] profesora Dujelle i knjigu "A Course in Number Theory and Cryptography" [4].

U trećem poglavlju se bavimo reprezentacijom konačnih polja pa nam trebaju osnovne definicije polinoma, operacija zbrajanja i umnoška nad njima, prstenom polinoma, ireducibilnosti i korijena polinoma. Pokazat ćemo kako u programskom paketu PARI/GP možemo reprezentirati polinome i raditi operacije nad njima. Dajemo dva teorema vezana za definirajuće ireducibilne polinome u konačnim poljima. U ovom poglavlju (i ostatku rada) nam je glavna literatura knjiga "Computational Number Theory" [1].

U četvrtom poglavlju implementiramo aritmetičke operacije nad konačnim poljima karakteristike 2 i 3. Objašnjavamo razliku između tih karakteristika i drugačiji pristup kod operacija. Pokazujemo algoritam za množenje te njegovo ubrzanje u vidu češalj metoda. Na kraju poglavlja dajemo algoritam za modularnu redukciju polinoma.

U petom poglavlju se bavimo algoritmima za inverz ireducibilnog polinoma - Euklidov inverz, njegovo ubrzanje - binarni inverz i varijantu binarnog inverza - gotovo inverz.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Poglavlje 1

Algebarske osnove

Algebra je jedna od fundamentalnih grana matematike. U ovom poglavlju definirat ćemo neke od osnovnih *algebarskih struktura* – grupe, prstene i polja.

1.1 Grupa

Definicija 1.1.1. *Neprazan skup $G = (G, \cdot)$, gdje je $\cdot : G \times G \to G$ binarna operacija, zove se **grupa** ako vrijede sljedeća svojstva:*

(i) $(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \forall x, y, z \in G$ (asocijativnost),

(ii) $(\exists e \in G): \quad e \cdot x = x \cdot e = x \quad \forall x \in G$ (neutralni element),

(iii) $(\forall x \in G)\left(\exists! x^{-1} \in G\right): \quad x \cdot x^{-1} = x^{-1} \cdot x = e$ (inverzni element).

*Element e, ili e_G ako želimo posebno naglasiti da je riječ o grupi G, zove se **neutralni element** grupe, ili kraće **neutral** grupe. Za zadani $x \in G$, element $x^{-1} \in G$ koji zadovoljava svojstvo (iii), zove se **inverzni element** od x, ili kraće **inverz** od x.*

Ako još vrijedi i svojstvo

$$x \cdot y = y \cdot x \quad \forall x, y \in G \quad \text{(komutativnost)},$$

onda kažemo da je G **komutativna (abelova) grupa**, a u suprotnom govorimo o **nekomutativnoj (neabelovoj) grupi**.

Napomena 1.1.2. *Ako imamo neki skup G na kojemu je definirana operacija $\cdot : G \times G \to G$, tj. za bilo koje $x, y \in G$ je uvijek i $x \cdot y \in G$, kažemo da je $(G, \cdot)$ **grupoid**. Grupoid u kojemu vrijedi i asocijativnost zove se **polugrupa**. Polugrupa koja ima jedinstven neutralni element zove se **monoid**. Jasno, monoid u kojemu postoji inverz svakog elementa je grupa.*

Naravno, kao i za grupe, možemo promatrati i (ne)komutativnost gornjih struktura. Tako govorimo o (ne)komutativnoj polugrupi, odnosno o (ne)komutativnom monoidu.

Definicija 1.1.3. *Za multiplikativnu grupu G kaže se da je **ciklička** ako postoji element $a \in G$ takav da za bilo koji $b \in G$ postoji neki cijeli broj j takav da vrijedi $b = a^j$. Takav element a nazivamo **generatorom** cikličke grupe i pišemo $G = \langle a \rangle$.*

Iz definicije odmah slijedi da je svaka ciklička grupa komutativna. Također primjećujemo da ciklička grupa može imati više od jednog elementa koji je generator grupe. Na primjer, u aditivnoj grupi $\mathbb{Z}$ i 1 i -1 su generatori.

S obzirom na "aditivnu" grupu ostataka cijelih brojeva nakon dijeljenja s n, nalazimo da tip operacije koja se tamo koristi dovodi do relacije ekvivalencije na skupu cijelih brojeva.

Definicija 1.1.4. *Podskup R od $S \times S$ naziva se **relacija ekvivalencije** na skupu S ako ima sljedeća tri svojstva:*

(i) $(s, s) \in R$ *za sve* $s \in S$ *(refleksivnost),*

(ii) ako $(s, t) \in R$*, tada* $(t, s) \in R$ *(simetrija),*

(iii) ako $(s, t), (t, u) \in R$*, tada* $(s, u) \in R$ *(tranzitivnost).*

Najočitiji primjer relacije ekvivalencije je relacija jednakosti. Važna je činjenica da relacija ekvivalencije R na skupu S inducira particiju S, odnosno reprezentaciju S kao unije nepraznih, međusobno disjunktnih podskupova od S. Ako sakupimo sve elemente od S ekvivalentne fiksnom $s \in S$, dobivamo klasu ekvivalencije od s, označenu s

$$[s] = \{t \in S : (s, t) \in R\}.$$

Skup svih različitih klasa ekvivalencije tada tvori željenu particiju S. Napominjemo da je $[s] = [t]$ upravo ako je $(s, t) \in R$.

Definicija 1.1.5. *Za proizvoljne cijele brojeve a, b i pozitivan cijeli broj n, kažemo da je a **kongruentan** s b po modulu n, i pišemo $a \equiv b \pmod{n}$, ako je razlika $a - b$ višekratnik n, odnosno ako je $a = b + kn$ za neki cijeli broj k.*

Lako se provjerava da je "kongruencija po modulu n" relacija ekvivalencije na skupu $\mathbb{Z}$ cijelih brojeva. Odnos je očito refleksivan i simetričan. Tranzitivnost također lako slijedi: ako $a = b + kn$ i $b = c + ln$ za neke cijele brojeve k i l, tada je $a = c + (k + l)n$, tako da je $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$ zajedno impliciraju $a \equiv c \pmod{n}$.

Razmotrimo sada klase ekvivalencije na koje relacija kongruencije po modulu n dijeli skup $\mathbb{Z}$. Ovo će biti skupovi

$$[0] = \{\ldots, -2n, -n, 0, n, 2n, \ldots\},$$
$$[1] = \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\},$$
$$\vdots$$
$$[n-1] = \{\ldots, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\}.$$

Možemo definirati na skupu $\{[0], [1], \ldots, [n-1]\}$ klasa ekvivalencije binarnu operaciju

$$[a] + [b] = [a+b], \tag{1.1}$$

gdje su a i b bilo koji elementi odgovarajućih skupova $[a]$ i $[b]$, a zbroj $a+b$ s desne strane je obični zbroj od a i b. Kako bismo pokazali da smo zapravo definirali operaciju, odnosno da je ova operacija dobro definirana - moramo potvrditi da je element slike para $([a], [b])$ jedinstveno određen s $[a]$ i $[b]$ sam i ni na koji način ne ovisi o predstavnicima a i b. Asocijativnost te operacije slijedi iz asocijativnosti običnog zbrajanja. Element identiteta je $[0]$, a inverz od $[a]$ je $[-a]$. Stoga elementi skupa $\{[0], [1], \ldots, [n-1]\}$ tvore grupu.

Definicija 1.1.6. *Grupa koju tvori skup* $\{[0], [1], \ldots, \{n-1]\}$ *klasa ekvivalencije modulo n s operacijom 1.1 naziva se grupa cijelih brojeva modulo n u oznaci* $\mathbb{Z}_n$.

$\mathbb{Z}_n$ je zapravo ciklička grupa s klasom ekvivalencije $[1]$ kao generatorom, a to je grupa reda n prema sljedećoj definiciji.

Definicija 1.1.7. *Grupa se naziva* ***konačnom*** *(beskonačnom) ako sadrži konačno (beskonačno) mnogo elemenata. Broj elemenata u konačnoj grupi naziva se njezin* ***red****. Za red konačne grupe G pisat ćemo* $|G|$.

Definicija 1.1.8. *Podskup H grupe G je* ***podgrupa*** *od G ako je H sama grupa u odnosu na operaciju od G. Podgrupe od G osim trivijalne podgrupe* $\{e\}$ *i same G nazivaju se* ***netrivijalne podgrupe*** *od G.*

Propozicija 1.1.9. *Za bilo koji fiksni a u grupi G, skup svih potencija od a je podgrupa od G.*

Definicija 1.1.10. *Podgrupa od G koja se sastoji od svih potencija elementa a od G naziva se* ***podgrupa koju generira*** *a i označava se s* $\langle a \rangle$*. Ova podgrupa je nužno ciklička. Ako je* $\langle a \rangle$ *konačan, tada se njegov red naziva redom elementa a. Inače se a naziva elementom beskonačnog reda.*

Dakle, a je konačnog reda k ako je k najmanji pozitivni cijeli broj takav da je $a^k = e$. Bilo koji drugi cijeli broj m s $a^m = e$ tada je višekratnik k. Ako je S neprazan podskup grupe G, tada se podgrupa H od G koja se sastoji od svih konačnih umnožaka potencija

elemenata iz S naziva podgrupa koju generira S, označava se s $H = \langle S \rangle$. Ako je $\langle S \rangle = G$, kažemo da S generira G, ili da G generira S.

Za pozitivan element n aditivne grupe $\mathbb{Z}$ cijelih brojeva, podgrupa $\langle n \rangle$ usko je povezana s pojmom kongruencije po modulu n, budući da je $a \equiv b \pmod{n}$ ako i samo ako je $a - b \in \langle n \rangle$. Stoga podgrupa $\langle n \rangle$ definira relaciju ekvivalencije na $\mathbb{Z}$.

1.2 Prsten

Definicija 1.2.1. *Neprazan skup $R = (R, +, \cdot)$ zovemo **prsten** ukoliko je za operacije zbrajanja $+ : R \times R \to R$ i množenja $\cdot : R \times R \to R$ ispunjeno sljedeće:*

- *$(R, +)$ je komutativna grupa, s neutralom $0 = 0_R$;*
- *$(R, \cdot)$ je polugrupa*
- *Vrijedi distributivnost "množenja prema zbrajanju", tj.*

$$\begin{aligned} x \cdot (y + z) &= x \cdot y + x \cdot z, \quad \forall x, y, z \in R, \\ (x + y) \cdot z &= x \cdot z + y \cdot z, \quad \forall x, y, z \in R. \end{aligned}$$

*Element $0 = 0_R$, neutral u grupi $(R, +)$, zvat ćemo **nula** prstena R. Ako postoji **jedinični element**, ili kraće **jedinica**, $1 = 1_R \in R$ takav da je*

$$1 \cdot x = x \cdot 1 = x, \quad \forall x \in R,$$

*onda kažemo da je R **prsten s jedinicom**. Prsten R je **komutativan prsten** ako je*

$$x \cdot y = y \cdot x, \quad \forall x, y \in R;$$

*inače govorimo o **nekomutativnom prstenu**.*

Primjer 1.2.2. *(1) Skup cijelih brojeva $\mathbb{Z}$ s običnim zbrajanjem i množenjem je komutativan prsten s jedinicom.*
(2) Skup svih funkcija $f, g : \mathbb{R} \to \mathbb{R}$ čini komutativan prsten s jedinicom, ako sumu $f + g$ i produkt $f \cdot g$ definiramo sa:

$$\begin{aligned} (f + g)(x) &= f(x) + g(x), \forall x \in \mathbb{R} \\ (f \cdot g)(x) &= f(x) \cdot g(x), \forall x \in \mathbb{R} \end{aligned}$$

(3) Skup svih 2×2 matrica s elementima iz $\mathbb{R}$ čini nekomutativan prsten s jedinicom obzirom na standardne operacije zbrajanja i množenja matrica.

Definicija 1.2.3. *Skup $S \subseteq R$, gdje je R neki prsten, je potprsten od R ako je $S = (S, +, \cdot)$ i sam prsten. Drugim riječima, S je* ***potprsten*** *od R ako vrijede sljedeća dva uvjeta:*

- $(\forall x, y \in S): \quad x - y \in S \quad$ ($(S, +)$ je grupa)
- $(\forall x, y \in S): \quad x \cdot y \in S \quad$ ($(S, \cdot)$ je grupoid).

Činjenicu da je S potprsten od R označavamo, analogno kao i kod grupa, sa

$$S \leq R.$$

Definicija 1.2.4. *Prsten R je* ***integralna domena****, ako je on komutativan prsten s jedinicom $1 \neq 0$, u kojem nema djelitelja nule, tj. vrijedi:*

$$x \cdot y = 0 \Rightarrow x = 0 \text{ ili } y = 0 \quad \forall x, y \in R.$$

Definicija 1.2.5. *Element $w \in R$, gdje je R prsten s jedinicom 1 je* ***invertibilan****, ako postoji $w' \in R$ takav da je*

$$w \cdot w' = w' \cdot w = 1$$

Oznaka koja se koristi:

$$R^{\times} := \text{grupa invertibilnih elementa u } R.$$

Sljedeći pojam je posebno važan u teoriji polja.

Definicija 1.2.6. *Neka je R prsten i pretpostavimo da postoji $m \in \mathbb{N}$ takav da je*

$$mx = 0, \quad \forall x \in R.$$

Definirajmo ***karakteristiku prstena*** *R sa*

$$\text{char } R := \text{ minimalan takav } m;$$

jasno, ako m uopće postoji. U suprotnom govorimo da je R karakteristike nula, i pišemo

$$\text{char } R = 0.$$

Definicija 1.2.7. *Podskup S prstena R naziva se* ***potprstenom*** *od R pod uvjetom da je S zatvoren prema operacijama zbrajanja i oduzimanja te tvori prsten prema tim operacijama.*

Definicija 1.2.8. *Podskup J prstena R naziva se* ***idealom*** *ako je J potprsten od R i za sve $a \in J$ i $r \in R$ imamo $ar \in J$ i $ra \in J$.*

Definicija 1.2.9. *Neka je R komutativni prsten. Kaže se da je ideal J od R **glavni** ako postoji $a \in R$ takav da je $J = (a)$. U ovom slučaju, J se također naziva glavnim idealom generiranim s a.*

Teorem 1.2.10. *Prsten $R \neq \{0\}$ pozitivne karakteristike koji ima jedinicu i nema djelitelja nule mora imati prosti broj za karakteristiku.*

Dokaz. Budući da R sadrži elemente različite od nule, R ima karakteristiku $n \geqslant 2$. Da n nije prosti broj, mogli bismo napisati $n = km$ s $k, m \in \mathbf{Z}, 1 < k, m < n$. Tada je $0 = n \cdot 1 = (km) \cdot 1 = (k \cdot 1)(m \cdot 1)$, a to implicira da je ili $k \cdot 1 = 0$ ili $m \cdot 1 = 0$ budući da R nema djelitelje nule. Slijedi da je ili $kr = (k \cdot 1)r = 0$ za sve $r \in R$ ili $mr = (m \cdot 1)r = 0$ za sve $r \in R$, u suprotnosti s definicijom karakteristike n. □

Teorem 1.2.11. *Neka je R komutativni prsten karakteristike p, gdje je p prost broj, tada slijedi*

$$(a + b)^{r^n} = a^{p^n} + b^{p^n} \quad i \quad (a - b)^{p^n} = a^{p^n} - b^{p^n}$$

za $a, b \in R$ i $n \in \mathbb{N}$.

Dokaz. Koristimo se činjenicom da vrijedi

$$\left(\begin{array}{c} p \\ i \end{array} \right) = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdot \cdots \cdot i} \equiv 0 \pmod{p} \quad , \forall i \in \mathbf{Z} \text{ gdje je } 0 < i < p.$$

Zatim po binomnom teoremu,

$$(a + b)^p = a^p + \left(\begin{array}{c} p \\ 1 \end{array} \right) a^{p-1}b + \cdots + \left(\begin{array}{c} p \\ p-1 \end{array} \right) ab^{p-1} + b^p = a^p + b^p,$$

i indukciji po n dovršavamo dokaz prvog identiteta. Ovim smo dobili

$$a^{p^n} = ((a - b) + b)^{p^n} = (a - b)^{p^n} + b^{p^n},$$

odnosno

$$(a - b)^{p^n} = a^{p^n} - b^{p^n}.$$

□

1.3 Polje

Definicija 1.3.1. *Prsten R je **tijelo**, ili **prsten s dijeljenjem**, ako je svaki nenul element u R invertibilan; tj. ako vrijedi*

$$R^\times = R\backslash\{0\}.$$

*Komutativno tijelo zovemo **polje**.*

Teorem 1.3.2. *Svaka konačna integralna domena je polje.*

Dokaz. Jedino što trebamo pokazati je da element a iz integralne domene, za koji vrijedi $a \neq 0$, ima multiplikativni inverz. Promatramo $a, a^2, a^3, \ldots$ Budući da ima samo konačno mnogo elemenata, moramo imati $a^m = a^n$ za neki $m < n$. Zatim $0 = a^m - a^n = a^m(1 - a^{n-m})$. Budući da nema djelitelja nule, moramo imati $a^m \neq 0$ i prema tome $1 - a^{n-m} = 0$, odnosno $1 = a\left(a^{n-m-1}\right)$ i pronašli smo multiplikativni inverz za a. □

Primjer 1.3.3. *(1) Prvi i osnovni primjeri polja, koji su fundamentalni objekti u svim granama matematike, su **polje racionalnih brojeva** $\mathbb{Q}$, **polje realnih brojeva** $\mathbb{R}$ i **polje kompleksnih brojeva** $\mathbb{C}$, gdje su operacije zbrajanja i množenja standardno definirane. Znamo da vrijedi $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.*
(2) Skup cijelih brojeva $\mathbb{Z}$ je integralna domena, ali ne i polje (u $\mathbb{Z}$ inverz imaju samo ± 1).
(3) Polja $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ su beskonačna jer sadržavaju beskonačno mnogo elemenata.

Definicija 1.3.4. *Neka je R komutativni prsten s jedinicom. Element $a \in R$ naziva se **djelitelj** od $b \in R$ ako postoji $c \in R$ takav da je $ac = b$. Za dva elementa $a, b \in R$ kaže se da su **pridruženi** ako postoji jedinica od R takva da je $a = b \cdot 1$. Element $c \in R$ naziva se **prostim** elementom ako nije jedinica i ako su mu djelitelji samo elementi pridruženi c. Ideal $P \neq R$ prstena R naziva se **prostim idealom** ako za $a, b \in R$ imamo $ab \in P$ samo ako $a \in P$ ili $b \in P$. Ideal $M \neq R$ od R naziva se **maksimalnim idealom** od R ako za bilo koji ideal J od R svojstvo $M \subseteq J$ implicira $J = R$ ili $J = M$. Nadalje, za R se kaže da je **domena glavnih ideala** ako je R integralna domena i ako je svaki ideal J od R glavni - to jest, ako postoji generirajući element a za J tako da je $J = (a) = \{ra : r \in R\}$.*

Teorem 1.3.5. *Neka je R komutativni prsten s jedinicom. Vrijedi:*

(i) Ideal M od R je maksimalni ideal ako i samo ako je R/M polje.

(ii) Ideal P od R je prosti ideal ako i samo ako je R/P integralna domena.

(iii) Svaki maksimalni ideal od R je prosti ideal.

(iv) Ako je R domena glavnih ideala, tada je $R/(c)$ polje ako i samo ako je c prosti element od R.

Dokaz ovog teorema se može naći u knjizi [5].

Poglavlje 2

Konačna polja

Definicija 2.0.1. *Polje koje sadrži konačno mnogo elemenata nazivamo* ***konačno polje****.*

Teorem 2.0.2. *Polje je nužno integralna domena.*

Dokaz. Budući da je polje komutativni prsten s jedinicom, da bismo pokazali da je svako polje integralna domena, trebamo samo dokazati da je polje bez djelitelja nule. Neka $\boldsymbol{F}$ bude bilo koje polje i neka $a, b \in F$ s $a \neq 0$ tako da je $ab = 0$. Neka je 1 jedinica od F. Budući da je $a \neq 0, a^{-1}$ postoji u $\boldsymbol{F}$, dakle

$$\begin{aligned} ab = 0 \Rightarrow & a^{-1}(ab) = a^{-1}0 \\ \Rightarrow & \left(a^{-1}a\right)b = 0 \\ \Rightarrow & 1 \cdot b = 0 \\ \Rightarrow & b = 0 \end{aligned}$$

Slično, ako je $b \neq 0$ tada se može pokazati da $ab = 0 \Rightarrow a = 0$. Dakle $ab = 0 \Rightarrow a = 0$ ili $b = 0$. Dakle, polje je nužno integralna domena. □

Propozicija 2.0.3. *Karakteristika konačnog polja je prost broj.*

Dokaz. Pretpostavimo suprotno, $\operatorname{char} F = m = uv$ gdje je $1 < u, v < m$ za neko konačno polje F. Cijeli brojevi m, u, v poistovjećuju se s elementima m_F, u_F, v_F od F. Prema svojstvu distributivnosti, imamo $0 = m_F = u_F v_F$. Prema definiciji, u_F i v_F nisu nula (u, v su manji od m). U prošlom teoremu smo dokazali da je polje integralna domena, tj. da umnožak dva elementa različita od nule ne može biti 0. Dakle, za m ne vrijedi produkt kao što je gore pretpostavljeno. Nadalje, ako je $m = 1$, tada je F nulti prsten (nije polje po definiciji). □

Najjednostavniji primjeri konačnih polja su prsteni $\mathbb{Z}_p$, gdje je p prost broj.

Propozicija 2.0.4. *Svako konačno polje je reda p^n za neki $p \in \mathbb{P}$ i $n \in \mathbb{N}$.*

Dokaz. Neka je konačno polje $\mathbb{F}$ reda q, u oznaci $\mathbb{F}_q$. $\mathbb{F}_q$ ne može biti karakteristike 0 pa neka je p karakteristika od $\mathbb{F}_q$. Tada $\mathbb{F}_q$ sadržava prosto polje $\mathbb{Z}/p\mathbb{Z}$, u oznaci $\mathbb{F}_p$. Nadalje, $\mathbb{F}_q$ je konačno dimenzionalni vektorski prostor nad $\mathbb{F}_p$. Neka je njegova dimenzija n, a $e_1, \ldots, e_n$ baza. Tada se svaki element $\alpha \in \mathbb{F}_q$ može prikazati u obliku linearne kombinacije $\alpha = \lambda_1 e_1 + \cdots + \lambda_n e_n$, gdje su $\alpha_i \in \mathbb{F}_p$. Dakle, svakom $\alpha \in \mathbb{F}_q$ možemo bijektivno pridružiti uređenu n-torku $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{F}_p)^n$. Stoga je $q = p^n$. □

Definicija 2.0.5. *Konačno polje reda $q = p^n$ označavamo s $\mathbb{F}_q = \mathbb{F}_{p^n}$. Ako je q prost (i $n = 1$), polje $\mathbb{F}_q = \mathbb{F}_p$ nazivamo **prosto polje**. Ako vrijedi $n > 1$, $\mathbb{F}_q$ zovemo **prošireno polje**.*

Za prost broj p, $\mathbb{F}_p$ i $\mathbb{Z}_p$ su isti algebarski objekt. Ako vrijedi $q = p^n$ i $n > 1$, $\mathbb{F}_q$ i $\mathbb{Z}_q$ su dva različita prstena. $\mathbb{F}_q$ je polje, svaki nenul element ima inverz. Dok $\mathbb{Z}_q$ nije polje. Vrijedi $\phi(p^n) = p^{n-1}(p-1)$, odnosno, $\mathbb{Z}_q$ sadrži $p^{n-1} - 1 > 0$ nenul, neinvertibilnih elementa kao $p, 2p, \ldots, \left(p^{n-1} - 1\right)p$.

U ostatku rada nam je p prost broj i vrijedi $q = p^n$ za neki $n \in \mathbb{N}$.

Teorem 2.0.6. *Za svako konačno polje $\mathbb{F}_q$ multiplikativna grupa $\mathbb{F}_q^*$ nenul elemenata od $\mathbb{F}_q$ je ciklička.*

Dokaz. Možemo pretpostaviti $q > 3$. Neka je $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ dekompozicija na proste faktore reda $h = q - 1$ grupe $\mathbb{F}_q^*$. Za svaki i, $1 \leqslant i \leqslant m$, polinom $x^{h/p_1} - 1$ ima najviše h/p_i korijena u $\mathbb{F}_q$. Budući da je $h/p_t < h$, slijedi da postoje elementi različiti od nule u $\mathbb{F}_q$ koji nisu korijeni ovog polinoma. Neka a_i bude takav element i neka je $b_i = a_i^{h/pp_i^j}$. Imamo $b_i^{p_i'} = 1$, stoga je red od b_i djelitelj od $p_i^{r'}$ i stoga je oblika $p_i^{s_i}$ s $0 \leqslant s_i \leqslant r_i$. S druge strane,

$$b_i^{p_i^{-1}} = a_i^{h/p_i} \neq 1,$$

pa je red od b_i jednak $p_i^{r_i}$. Tvrdimo da element $b = b_1 b_2 \cdots b_m$ ima red h. Pretpostavimo, naprotiv, da je red od b pravi djelitelj od h i stoga je djelitelj barem jednog od m cijelih brojeva h/p_i, $1 \leqslant i \leqslant m$, recimo od h/p_1. Onda imamo

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1}.$$

Sada ako $2 \leqslant i \leqslant m$, tada $p_i^{r_i}$ dijeli h/p_1, a time i $b_i^{h/p_1} = 1$. Prema tome $b_1^{h/p_1} = 1$. Ovo implicira da red od b_1 mora dijeliti h/p_1, što je nemoguće jer je red od b_1 jednak $p_1^{r_1}$. Dakle, F_q^* je ciklička grupa s generatorom b. □

2.1 Mali Fermatov teorem za konačna polja

Teorem 2.1.1. ***Mali Fermatov teorem za*** $\mathbb{F}_q$
Neka je $\alpha \in \mathbb{F}_q$*. Tada imamo* $\alpha^q = \alpha$*. Nadalje, ako je* $\alpha \neq 0$*, tada je* $\alpha^{q-1} = 1$*.*

Dokaz. Prvo, uzmimo $\alpha \neq 0$ i neka $\alpha_1, \ldots, \alpha_{q-1}$ budu svi elementi od $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$. Tada je $\alpha\alpha_1, \ldots, \alpha\alpha_{q-1}$ permutacija $\alpha_1, \ldots, \alpha_{q-1}$. Dakle vrijedi

$$\prod_{i=1}^{q-1} \alpha_i = \prod_{i=1}^{q-1} (\alpha\alpha_i) = \alpha^{q-1} \prod_{i=1}^{q-1} \alpha_i.$$

Dobivamo $\alpha^{q-1} = 1$ odnosno $\alpha^q = \alpha$. Za $\alpha = 0$, imamo $0^q = 0$. □

Vrlo važna posljedica ovog teorema je sljedeći korolar.

Korolar 2.1.2. *Polinom* $x^q - x \in \mathbb{F}_p[x]$ *rastavlja se na linearne faktore nad* $\mathbb{F}_q$ *kao* $x^q - x = \prod_{\alpha \in \mathbb{F}_q}(x - \alpha)$*.*

Propozicija 2.1.3. *Neka je* $q = p^n$ *i* d *pozitivan djelitelj od* n*. Tada* $\mathbb{F}_q$ *sadrži jedinstveno polje veličine* $\mathbb{F}_{p^d}$*. Nadalje, element* $\alpha \in \mathbb{F}_q$ *pripada ovom polju ako i samo ako je* $\alpha^{p^d} = \alpha$*.*

Dokaz. Razmotrimo skup $E = \left\{\alpha \in \mathbb{F}_q \mid \alpha^{p^d} = \alpha\right\}$. Lako je provjeriti da E zadovoljava sve aksiome polja i da E sadrži točno p^d elemenata. □

Poglavlje 3

Reprezentacija konačnih polja

Prosto polje $\mathbb{F}_p$ je isto kao i $\mathbb{Z}_p$, odnosno, aritmetika $\mathbb{F}_p$ može se izvesti kao cjelobrojna aritmetika po modulu prostog broja p. Mi se nećemo baviti modularnom aritmetikom nego se koncentriramo na proširena polja.

3.1 Polinomi

Definicija 3.1.1. *Za dva polinoma*

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{i} \quad g(x) = \sum_{i=0}^{n} b_i x^i$$

definiramo ***zbroj*** $f(x) + g(x)$ *kao*

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i)\, x^i.$$

Definicija 3.1.2. *Za dva polinoma*

$$f(x) = \sum_{i=0}^{n} a_n x^i \quad \text{i} \quad g(x) = \sum_{j=0}^{m} b_j x^j$$

definiramo ***umnožak*** $f(x)g(x)$ *kao*

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \quad \text{gdje je } c_k = \sum_{\substack{i+j-k \\ 0 \leqslant i \leqslant n, 0 \leqslant j \leqslant m}} a_i b_j.$$

Definicija 3.1.3. *Prsten koji formiraju polinomi nad R s operacijama zbrajanja i množenja naziva se* ***prsten polinoma nad*** *R i označava se s* $R[x]$.

Definicija 3.1.4. *Neka je* $f(x) = \sum_{i=0}^{n} a_i x^i$ *polinom nad R koji nije nul-polinom, tako da možemo pretpostaviti* $a_n \neq 0$. *Tada se* a_n *naziva* ***vodećim koeficijentom*** *od* $f(x)$, *a* a_0 ***konstantnim članom***, *dok se n naziva* ***stupnjem*** *od* $f(x)$, *u simbolima* $n = \deg(f(x)) = \deg(f)$. *Prema konvenciji, postavljamo* $\deg(0) = -\infty$. *Polinomi stupnja* $\leqslant 0$ *nazivaju se* ***konstantni polinomi***. *Ako R ima jedinicu 1 i ako je vodeći koeficijent od* $f(x)$ *jednak 1, tada se* $f(x)$ *naziva* ***normirani polinom***.

Teorem 3.1.5. *Neka je R prsten. Vrijedi:*

(i) $R[x]$ *je komutativno ako i samo ako je R komutativan.*

(ii) $R[x]$ *je prsten s jedinicom ako i samo ako R ima jedinicu.*

(ii) $R[x]$ *je integralna domena ako i samo ako je R integralna domena.*

Teorem 3.1.6. *Neka je* $g \neq 0$ *polinom u* $F[x]$. *Tada za bilo koji* $f \in F[x]$ *postoje polinomi* $q, r \in F[x]$ *takvi da je* $f = qg + r$, *gdje je* $\deg(r) < \deg(g)$.

Definicija 3.1.7. *Kaže se da je polinom* $p \in F[x]$ ***ireducibilan*** *nad F (ili ireducibilan u* $F[x]$, *ili prost u* $F[x]$*) ako p ima pozitivan stupanj i* $p = bc$ *gdje* $b, c \in F[x]$ *implicira da je ili b ili c konstantan polinom.*

Lema 3.1.8. *Ako ireducibilan polinom p u* $F[x]$ *dijeli produkt* $f_1 \cdots f_m$ *polinoma u* $F[x]$, *tada je barem jedan od faktora* f_j *djeljiv sa p.*

Dokaz. Budući da p dijeli $f_1 \cdots f_m$, dobivamo identitet $(f_1 + (p)) \cdots (f_m + (p)) = 0 + (p)$ u prstenu polinoma $F[x]/(p)$. Sada je $F[x]/(p)$ polje prema teoremu 1.3.5, pa je $f_j + (p) = 0 + (p)$ za neki j; odnosno p dijeli f_j. □

Definicija 3.1.9. *Element* $b \in F$ *naziva se* ***korijen*** *(ili nula) polinoma* $f \in F[x]$ *ako je* $f(b) = 0$.

Važnu vezu između korijena i djeljivosti daje sljedeći teorem.

Teorem 3.1.10. *Element* $b \in F$ *je korijen polinoma* $f \in F[x]$ *ako i samo ako* $x - b$ *dijeli* $f(x)$.

Dokaz. Koristimo teorem 3.1.6 da zapišemo $f(x) = q(x)(x - b) + c$ s $q \in F[x]$ i $c \in F$. Zamjenom b s x, dobivamo $f(b) = c$, dakle $f(x) = q(x)(x - b) + f(b)$. Teorem sada slijedi iz ovog identiteta. □

Za svaki $p \in \mathbb{P}$ i $n \in \mathbb{N}$, postoji barem jedan ireducibilni polinom stupnja n u $\mathbb{F}_p[x]$. Neka je $F = \mathbb{F}_p$ i $f(x) \in F[x]$ ireducibilni polinom stupnja $n \geqslant 2$.

Zamislimo da je θ korijen od $f(x)$ u najmanjem polju K koje sadrži $F = \mathbb{F}_p$. Tada, svaki polinomijalni izraz $t(\theta)$ sa $t(x) \in \mathbb{F}_p[x]$ mora biti u K. Imamo $f(\theta) = 0$ i $\deg f = n$. Dakle, θ^n se može izraziti kao F-linearna kombinacija od $1, \theta, \theta^2, \ldots, \theta^{n-1}$. Također se može izraziti i $\theta^{n+1} = \theta \times \theta^n$. Odnosno, θ^k za sve $k \geqslant n$ se može izraziti kao F-linearna kombinacija od $1, \theta, \theta^2, \ldots, \theta^{n-1}$. Također, ako je stupanj $t(x) \geqslant n$, još uvijek možemo izraziti $t(\theta)$ kao polinomijalni izraz (u θ) stupnja manjeg od n.

Uzmimo sada neki nenul element $t(\theta)$ stupnja manjeg od n. Kako je $f(x)$ ireducibilan stupnja n, imamo $\mathrm{NZD}(t(x), f(x)) = 1$. Dakle, po Bézoutovom teoremu za polinome, postoje $u(x), v(x) \in F[x]$ takvi da $u(x)t(x) + v(x)f(x) = 1$. Kako vrijedi $f(\theta) = 0$, imamo $u(\theta)t(\theta) = 1$, odnosno, $t(\theta)^{-1} = u(\theta)$. Ako je $u(x)$ stupnja $\geqslant n$, reduciramo $u(\theta)$ do polinoma θ stupnja manjeg od n. Slijedi da K treba sadržavati samo polinomijalne izraze oblika $t(\theta)$ sa $t(x) \in F[x]$ i $\deg t(x) < n$.

Neka su $s(\theta), t(\theta)$ polinomi stupnja manjeg od n. Tada je i polinom $r(x) = s(x) - t(x)$ stupnja manjeg od n. Pretpostavimo da je $r(x) \neq 0$ i $r(\theta) = 0$. Ali tada θ je korijen od $r(x)$ i $f(x)$. Kako je $\deg r(x) < n$ i $f(x)$ je ireducibilan, imamo $\gcd(r(x), f(x)) = 1$, odnosno θ je korijen od 1, što nije moguće. Slijedi da $r(\theta) = 0$ ako i samo ako $r(x) = 0$, odnosno, $s(x) = t(x)$. To nam govori da različiti polinomi $s(x), t(x)$ stupnja manjeg od n predstavljaju različite elemente $s(\theta), t(\theta)$ od K. Dakle, K se može prikazati skupom

$$K = \{t(\theta) \mid t(x) \in F[x], \deg t(x) < n\}.$$

Polinom $t(x)$ ovog oblika ima n koeficijenata (od $1, x, x^2, \ldots, x^{n-1}$) i svaki od tih koeficijenata može biti bilo koji od p brojeva iz $F = \mathbb{F}_p$. Također, red od K je p^n, dakle, K je konkretna realizacija polja $\mathbb{F}_q = \mathbb{F}_{p^n}$. Ovu reprezentaciju zovemo polinomna reprezentacija od $\mathbb{F}_q$ nad $\mathbb{F}_p$, zato što svaki element od K je $\mathbb{F}_p$-linearna kombinacija od $1, \theta, \theta^2, \ldots, \theta^{n-1}$. Zapisujemo to kao $K = F(\theta)$.

$\mathbb{F}_q$ je n-dimenzionalni vektorski prostor nad $\mathbb{F}_p$. Bilo koji skup od n elemenata $\theta_0, \theta_1, \ldots, \theta_{n-1}$ čini $\mathbb{F}_p$-bazu od $\mathbb{F}_q$ ako i samo ako ti elementi su linearno neovisni u $\mathbb{F}_p$. Elementi $1, \theta, \theta^2, \ldots, \theta^{n-1}$ čine jednu takvu bazu.

Znači, za predstavljanje proširenog polja $\mathbb{F}_q = \mathbb{F}_{p^n}$, potreban nam je ireducibilni polinom $f(x)$ stupnja n u $\mathbb{F}_p[x]$.

Normalni elementi

Koncept multiplikativnog reda modulo p može se generalizirati za $\mathbb{F}_q$.

Definicija 3.1.11. *Neka je $\alpha \in \mathbb{F}_q, \alpha \neq 0$. Najmanji prirodni broj e za koji je $\alpha^e = 1$ naziva se red od α i označava se s* $\operatorname{ord}\alpha$. *Prema Malom Fermatovom teoremu za $\mathbb{F}_q$ 2.1.1, imamo* $\operatorname{ord}\alpha \mid (q-1)$. *Ako je* $\operatorname{ord}\alpha = q-1$, *tada se α naziva* ***primitivnim elementom*** *$\mathbb{F}_q$. Ako je $\mathbb{F}_q = \mathbb{F}_p(\theta)$, gdje je θ korijen ireducibilnog polinoma $f(x) \in \mathbb{F}_p[x]$ i ako je θ primitivni element od $\mathbb{F}_q$, $f(x)$ nazivamo* ***primitivnim polinomom****.*

Neka je $\mathbb{F}_q = \mathbb{F}_p(\theta)$, gdje je θ korijen ireducibilnog polinoma $f(x) \in \mathbb{F}_p[x]$ stupnja n. Budući da $f(x)$ ima korijen θ u $\mathbb{F}_q$, polinom više nije ireducibilan u $\mathbb{F}_q[x]$. Ali što se događa s drugih $n-1$ korijena od $f(x)$?

Kako bismo odgovorili na ovo pitanje, prvo promatramo proširenje $\mathbb{R}$ pridruživanjem korijena i od x^2+1. Drugi korijen ovog polinoma je $-i$ koji je uključen u $\mathbb{C}$. Stoga se polinom x^2+1 faktorizira na linearne faktore nad $\mathbb{C}$ kao $x^2+1 = (x-\mathrm{i})(x+\mathrm{i})$. Budući da je definirajući polinom drugog stupnja i ima jedan korijen u proširenju, drugi korijen također mora biti u tom proširenju.

Proširimo sada polje $\mathbb{Q}$ korijenom θ polinoma x^3-2. Tri korijena ovog polinoma su $\theta_0 = 2^{1/3}$, $\theta_1 = 2^{1/3}e^{\mathrm{i}2\pi/3}$ i $\theta_2 = 2^{1/3}e^{\mathrm{i}4\pi/3}$. Uzmimo $\theta = \theta_0$. Budući da je ovaj korijen realan broj, njegovo pridruživanje $\mathbb{Q}$ daje polje sadržano u $\mathbb{R}$. S druge strane, korijeni θ_1, θ_2 su kompleksni brojevi, to jest, $\mathbb{Q}(\theta)$ ne sadrži θ_1, θ_2. Vrijedi $x^3-2 = \left(x-2^{1/3}\right)\left(x^2+2^{1/3}x+2^{2/3}\right)$, pri čemu je drugi faktor ireducibilan.

Gornja dva primjera ilustriraju da proširenje može, ali i ne mora sadržavati sve korijene definirajućeg polinoma. Koncentrirajmo se sada na konačna polja. Zapišimo $f(x)$ eksplicitno kao

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

sa svakim $a_i \in \mathbb{F}_p$. Imamo $f(x)^p = a_0^p + a_1^p x^p + a_2^p x^{2p} + \cdots + a_n^p x^{np}$. Prema Malom Fermatovom teoremu 2.1.1, $a_i^p = a_i$ u $\mathbb{F}_p$ i tada $f(x)^p = a_0 + a_1x^p + a_2x^{2p} + \cdots + a_nx^{np} = f(x^p)$. Ako uzmemo $x = \theta$ dobijemo $f(\theta^p) = f(\theta)^p = 0^p = 0$, odnosno θ^p je opet korijen od $f(x)$. Nadalje, $\theta^p \in \mathbb{F}_q$. Isto tako možemo tvrditi da $\theta^{p^2} = (\theta^p)^p$, $\theta^{p^3} = \left(\theta^{p^2}\right)^p, \ldots$ su korijeni od $f(x)$ i leže u $\mathbb{F}_q$. Može se pokazati da korijeni $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$ od $f(x)$ su u parovima različiti i tako moraju biti svi korijeni od $f(x)$. Drugim riječima, $f(x)$ se faktorizira na linearne faktore preko $\mathbb{F}_q$:

$$f(x) = a_n(x-\theta)(x-\theta^p)\left(x-\theta^{p^2}\right)\cdots\left(x-\theta^{p^{n-1}}\right).$$

Definicija 3.1.12. *Elementi θ^{p^i} za $i = 0, 1, 2, \ldots, n-1$ nazivaju se* ***konjugati*** *od θ. Ako su $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$ linearno neovisni nad $\mathbb{F}_p$, θ se naziva* ***normalnim elementom*** *od $\mathbb{F}_q$,*

a $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$ ***normalna baza*** *od* $\mathbb{F}_q$ *preko* $\mathbb{F}_p$*. Ako je normalni element* θ *također primitivni element od* $\mathbb{F}_q$*,* θ *nazivamo* ***primitivnim normalnim elementom****, a* $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$ ***primitivna normalna baza****.*

Najmanji polinomi

Konjugati od α su $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{t-1}}$, gdje je t je najmanji pozitivni cijeli broj za koji je $\alpha^{p^t} = \alpha$. Polinom

$$f_\alpha(x) = (x-\alpha)\,(x-\alpha^p)\left(x-\alpha^{p^2}\right)\cdots\left(x-\alpha^{p^{t-1}}\right)$$

je ireducibilan polinom u $\mathbb{F}_p[x]$. $f_\alpha(x)$ zovemo **minimalni polinom** od α nad $\mathbb{F}_p$, a t se naziva **stupanj** od α. Element α je korijen polinoma $g(x) \in \mathbb{F}_p[x]$ ako i samo ako $f_\alpha(x) \mid g(x)$ u $\mathbb{F}_p[x]$.

Definicija 3.1.13. *Element* $\alpha \in \mathbb{F}_{p^n}$ *naziva se* ***normalnim*** *ako* $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$ *su linearno neovisni o* $\mathbb{F}_p$*. Ako je stupanj od* α *djelitelj od n, ti elementi ne mogu biti linearno neovisni. Dakle, nužan uvjet da* α *bude normalan je da* α *ima stupanj n. Ako je* α *normalni element od* $\mathbb{F}_q$*, baza* $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$ *se naziva* ***normalnom bazom*** *od* $\mathbb{F}_{p^n}$ *nad* $\mathbb{F}_p$*. Ako je uz to* α *primitivan, naziva se* ***primitivni normalni element*** *od* $\mathbb{F}_{p^n}$*, a baza* $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$ *se naziva* ***primitivna normalna baza****.*

Teorem 3.1.14. *Za svaki* $p \in \mathbb{P}$ *i* $n \in \mathbb{N}$*, proširenje* $\mathbb{F}_{p^n}$ *sadrži normalan element. Nadalje, za svaki* $p \in \mathbb{P}$ *i* $n \in \mathbb{N}$*, postoji primitivni normalni element u* $\mathbb{F}_{p^n}$*.*

Propozicija 3.1.15. *Uzmimo* $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$*, gdje je* θ *korijen normiranog ireducibilnog polinoma* $f(x) \in \mathbb{F}_p[x]$ *(stupnja n). Promotrimo polinom*

$$g(x) = \frac{f(x)}{(x-\alpha)f'(\alpha)} \in \mathbb{F}_{p^n}[x],$$

gdje je $f'(x)$ *derivacija od* $f(x)$*. Tada postoji najmanje* $p - n(n-1)$ *elemenata a u* $\mathbb{F}_p$*, za koje je* $g(a)$ *normalan element od* $\mathbb{F}_{p^n}$ *preko* $\mathbb{F}_p$*.*

3.2 Polinomna reprezentacija

Primjer 3.2.1. *Pogledajmo polinomnu reprezentaciju* $\mathbb{F}_4 = \mathbb{F}_{2^2}$. *Polinomi stupnja 2 u* $\mathbb{F}_2[x]$ *su* $x^2, x^2 + x, x^2 + 1$ *i* $x^2 + x + 1$. *Kako vrijedi* $x^2 + 1 \equiv (x + 1)^2 \pmod 2$, *slijedi da je* $x^2 + 1$ *reducibilan, dok su prva dva očito također reducibilni. Polinom* $x^2 + x + 1$ *je ireducibilan, uzmimo ga kao definirajući polinom i neka je*

$$\mathbb{F}_4 = \mathbb{F}_2(\theta) = \{a_1\theta + a_0 \mid a_1, a_0 \in \{0, 1\}\}, \qquad \text{gdje je } \theta^2 + \theta + 1 = 0.$$

Elementi od $\mathbb{F}_4$ *su* $0, 1, \theta, \theta + 1$.

$+$	0	1	θ	$\theta+1$
0	0	1	θ	$\theta+1$
1	1	0	$\theta+1$	θ
θ	θ	$\theta+1$	0	1
$\theta+1$	$\theta+1$	θ	1	0

Tablica 3.1: Zbrajanje u $\mathbb{F}_4$

$\cdot$	0	1	θ	$\theta+1$
0	0	0	0	0
1	0	1	θ	$\theta+1$
θ	0	θ	$\theta+1$	1
$\theta+1$	0	$\theta+1$	1	θ

Tablica 3.2: Množenje u $\mathbb{F}_4$

Uzmimo elemente θ *i* $\theta + 1$. *Vrijedi* $\theta + (\theta + 1) = 2\theta + 1 = 1$ *modulo 2 i* $\theta(\theta + 1) = \theta^2 + \theta = \left(\theta^2 + \theta + 1\right) + 1 = 1$. *U bilo kojem prstenu karakteristike dva, oduzimanje je jednako zbrajanju* (*jer je* $-1 = 1$).

Primjer 3.2.2. *Rijndael*[1] *(Advanced Encryption Standard*[2]*), je kriptografska šifra čiji rad je baziran na aritmetici polja* $\mathbb{F}_{256} = \mathbb{F}_{2^8}$, *određen je ireducibilnim polinomom* $x^8 + x^4 + x^3 + x + 1$.

[1] Dobio ime po belgijskim kriprografima koji su ga razvili Joan Daemen i Vincent Rijmen.

[2] Skraćeno AES, je specifikacija za šifriranje elektroničkih podataka i usvojen je 26. studenog 2001. od strane američkog NIST-a (Nacionalnog instituta za standarde i tehnologiju).

Primjer 3.2.3. *Pogledajmo konačno polje karakteristike veće od 2, npr.* $\mathbb{F}_9 = \mathbb{F}_{3^2}$ *karakteristike 3. Kako 2 nije kvadratni ostatak modulo 3, polinom* $x^2 - 2$ *je ireducibilan u* $\mathbb{F}_3[x]$. *Ali* $-2 \equiv 1 \pmod 3$, *dakle uzmimo definirajući polinom* $f(x) = x^2 + 1$. *Vrijedi*

$$\mathbb{F}_9 = \mathbb{F}_3(\theta) = \{a_1\theta + a_0 \mid a_1, a_0 \in \{0, 1, 2\}\}, \text{ gdje je } \theta^2 + 1 = 0.$$

+	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
0	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
1	1	2	0	$\theta+1$	$\theta+2$	θ	$2\theta+1$	$2\theta+2$	2θ
2	2	0	1	$\theta+2$	θ	$\theta+1$	$2\theta+2$	2θ	$2\theta+1$
θ	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$	0	1	2
$\theta+1$	$\theta+1$	$\theta+2$	θ	$2\theta+1$	$2\theta+2$	2θ	1	2	0
$\theta+2$	$\theta+2$	θ	$\theta+1$	$2\theta+2$	2θ	$2\theta+1$	2	0	1
2θ	2θ	$2\theta+1$	$2\theta+2$	0	1	2	θ	$\theta+1$	$\theta+2$
$2\theta+1$	$2\theta+1$	$2\theta+2$	2θ	1	2	0	$\theta+1$	$\theta+2$	θ
$2\theta+2$	$2\theta+2$	2θ	$2\theta+1$	2	0	1	$\theta+2$	θ	$\theta+1$

Tablica 3.3: Zbrajanje u $\mathbb{F}_9$

·	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
2	0	2	1	2θ	$2\theta+2$	$2\theta+1$	θ	$\theta+2$	$\theta+1$
θ	0	θ	2θ	2	$\theta+2$	$2\theta+2$	1	$\theta+1$	$2\theta+1$
$\theta+1$	0	$\theta+1$	$2\theta+2$	$\theta+2$	2θ	1	$2\theta+1$	2	θ
$\theta+2$	0	$\theta+2$	$2\theta+1$	$2\theta+2$	1	θ	$\theta+1$	2θ	2
2θ	0	2θ	θ	1	$2\theta+1$	$\theta+1$	2	$2\theta+2$	$\theta+2$
$2\theta+1$	0	$2\theta+1$	$\theta+2$	$\theta+1$	2	2θ	$2\theta+2$	θ	1
$2\theta+2$	0	$2\theta+2$	$\theta+1$	$2\theta+1$	0	2	$\theta+2$	1	2θ

Tablica 3.4: Množenje u $\mathbb{F}_9$

3.3 Konačna polja u programskom paketu PARI/GP

PARI/GP je široko korišten računalni algebarski sustav dizajniran za brza izračunavanja u teoriji brojeva. Nama će koristiti za aritmetiku nad proširenim poljima $\mathbb{F}_q = \mathbb{F}_{p^n}$. To podrazumijeva dva tipa modularne aritmetike. Prvo, svi polinomijalni koeficijenti su reducirani modulo p, odnosno, aritmetika nad koeficijentima je modularna aritmetika od $\mathbb{Z}_p$. Drugo, aritmetika od $\mathbb{F}_q$ je polinomijalna aritmetika od $\mathbb{Z}_p[x]$ modulo definirajućim polinomom $f(x)$.

Pokažimo kako reprezentirati $\mathbb{F}_4$ iz Primjera 3.2.1. Prvo nam treba polinom $f(x)$.

```
? f = Mod(1,2)*x^2+Mod(1,2)*x+Mod(1,2)
%1 = Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2)
```

Sada uzmimo dva elementa od $\mathbb{F}_4$ kao dva polinoma iz $\mathbb{F}_2[x]$ modulo $f(x)$.

```
? a = Mod(Mod(1,2)*x, f)
%2 = Mod(Mod(1, 2)*x, Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2))
? b = Mod(Mod(1,2)*x+Mod(1,2), f)
%3 = Mod(Mod(1, 2)*x + Mod(1, 2), Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2))
```

Sada možemo odraditi aritmetičke operacije nad a i b.

```
? a + b
%4 = Mod(Mod(1, 2), Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2))
? a - b
%5 = Mod(Mod(1, 2), Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2))
? a * b
%6 = Mod(Mod(1, 2), Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2))
? a / b
%7 = Mod(Mod(1, 2)*x + Mod(1, 2), Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2))
? a^(-1)
%8 = Mod(Mod(1, 2)*x + Mod(1, 2), Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2))
? a^4
%9 = Mod(Mod(1, 2)*x, Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2))
```

Ako želimo imati malo pojednostavljeni prikaz, recimo bez $f(x)$ moramo iskoristiti **lift()**. Isto tako, ako ne želimo vidjeti ni **Mod** opet iskoristimo **lift()**.

```
? lift(a + b)
%10 = Mod(1, 2)
? lift(lift(a + b))
%11 = 1
? lift(lift(a * b))
%12 = 1
? lift(lift(a^4))
%13 = x
```

3.4 Odabir definirajućeg polinoma

Definicija 3.4.1. *Neka su $f, g : D \to \mathbb{R}$ realne funkcije na odozgo neograničenom podskupu $D \subseteq \mathbb{R}$.*

(i) f nije većeg reda veličine od g, ili f ne raste brže od g, u oznaci

$$f(x) \in O(g(x)) \quad (x \to \infty),$$

ako postoje realna konstanta $C > 0$ i $x_0 \in D$, takvi da je $\forall x > x_0$

$$|f(x)| < C|g(x)|$$

(ii) f je istog reda veličine kao i g, ili f raste istom brzinom kao i g, u oznaci

$$f(x) \in \Theta(g(x)) \quad (x \to \infty),$$

ako postoje realne konstante $c_1 > 0, c_2 > 0$, i $x_0 \in D$, takvi da je $\forall x > x_0$

$$c_1|g(x)| < |f(x)| < c_2|g(x)|$$

Ireducibilni polinom $f(x) \in \mathbb{F}_p[x]$ koji se koristi za definiranje proširenog polja $\mathbb{F}_{p^n}$ ima utjecaja na vrijeme izvođenja aritmetičkih operacija u $\mathbb{F}_{p^n}$. Množenje u $\mathbb{F}_{p^n}$ je množenje u $\mathbb{F}_p[x]$ dvaju polinoma stupnjeva manjih od n, nakon čega slijedi redukcija po modulu $f(x)$. Korak redukcije uključuje dugo dijeljenje polinoma stupnja $\leqslant 2n - 2$ polinomom stupnja n. Jednostavna implementacija tog dijeljenja može potrajati $\Theta\left(n^2\right)$ vremena. Ako $f(x)$ ima samo nekoliko koeficijenata različitih od nule, ovaj korak redukcije može biti značajno brži, jer je potrebno prilagoditi samo nekoliko koeficijenata u svakom koraku dijeljenja polinoma. Zato su nam jako zanimljivi polinomi u $\mathbb{F}_p[x]$ s točno 2, 3, 4 i 5 članova koji

nisu 0. Oni dovode do vremena reda O(n) za korak redukcije. Ireducibilni binom u $\mathbb{F}_p[x]$ mora biti oblika $x^n + a$ s $a \in \mathbb{F}_p^*$. Možemo karakterizirati sve vrijednosti a za koje je ovaj polinom ireducibilan.

Teorem 3.4.2. *Binom $x^n + a \in \mathbb{F}_p[x]$ je ireducibilan ako i samo ako su zadovoljena oba sljedeća uvjeta:*
(1) Svaki prosti faktor od n mora dijeliti $\operatorname{ord}_p(-a)$*, ali ne i* $(p-1)/\operatorname{ord}_p(-a)$.
(2) Ako je $n \equiv 0 \pmod 4$*, tada je* $p \equiv 1 \pmod 4$.

Oba ova uvjeta su previše restriktivna. Na primjer, nemamo ireducibilne binome stupnja $4k$ nad prostim poljem reda $4l + 3$. Stoga je preporučljivo proučavati ireducibilne trinome $x^n + ax^k + b$ s $1 \leqslant k \leqslant n-1$ i $a, b \in \mathbb{F}_p^*$. Nisu poznate potpune karakterizacije ireducibilnih trinoma nad svim prostim poljima $\mathbb{F}_p$. Ipak, dostupni su neki djelomični rezultati. Na primjer, sljedeći rezultat je koristan kada $p \gg n$.

Teorem 3.4.3. *Broj ireducibilnih trinoma u $\mathbb{F}_p[x]$ oblika $x^n + x + b$ (s $b \in \mathbb{F}_p^*$) je asimptotski jednako p/n.*

Ovaj rezultat pokazuje da nakon isprobavanja O(n) slučajnih vrijednosti od b, očekujemo da ćemo dobiti ireducibilan trinom oblika $x^n + x + b$. Izbor $k = 1$ u prošlom teoremu posebno je pogodan za učinkovite implementacije. Međutim, ako je p malen, nema mnogo izbora za b da nasumično pretraživanje uspije s velikom vjerojatnošću. U tom slučaju, moramo pokušati s drugim vrijednostima k. Za svako konačno polje $\mathbb{F}_p$ i svaki stupanj n, ireducibilan binom, trinom ili kvadrinom možda neće postojati. Međutim, zanimljiva je sljedeća slutnja.

Slutnja 3.4.4. *Za bilo koje konačno polje $\mathbb{F}_q$ s $q \geqslant 3$ i za bilo koje $n \in \mathbb{N}$, postoji ireducibilan polinom u $\mathbb{F}_q[x]$ sa stupnjem n i s najviše četiri člana različita od nule.*

Poglavlje 4

Efikasne implementacije operacija

4.1 Reprezentacija elemenata

U prošlom poglavlju smo pokazali da nam za reprezentaciju proširenog polja $\mathbb{F}_q = \mathbb{F}_{p^n}$ treba definirajući polinom $f(x) \in \mathbb{F}_p[x]$ stupnja n. On nam služi kao modulo za sve operacije. Element $\alpha \in \mathbb{F}_q$ je polinom stupnja manjeg od n i možemo ga reprezentirati pomoću n njegovih koeficijenata, gdje je svaki od njih cijeli broj modulo p. Jedino što nam preostaje je napisati aritmetičke metode za manipulaciju tih polinoma.

Slučaj kada je $p = 2$ nam je najlakši pa ćemo prvo promatrati polja karakteristike 2. Element od $\mathbb{F}_2$ je bit pa slijedi da je element od $\mathbb{F}_{2^n}$ polje od n bitova. Radi lakšeg pisanja organizirat ćemo više bitova u riječi, uobičajeno je uzimati 32 ili 64 za veličinu riječi.

Primjer 4.1.1. *Za ilustraciju ću uzeti još manju riječ (samo 8 bitova će predstavljati jednu riječ). Promatramo $\mathbb{F}_{2^{19}}$ kao $\mathbb{F}_2(\theta)$, gdje je θ korijen ireducibilnog polinoma $f(x) = x^{19} + x^5 + x^2 + x + 1$. Element od $\mathbb{F}_{2^{19}}$ je polinom oblika*

$$a_{18}\theta^{18} + a_{17}\theta^{17} + \cdots + a_1\theta + a_0,$$

gdje je svaki $a_i \in \{0, 1\}$. Niz koeficijenata $a_{18}a_{17}\ldots a_1a_0$ reprezentira ovaj element. Kako imamo 19 bitova, a riječ je veličine w, treba nam tri riječi veličine $w = 8$ bita za taj niz. To zapisujemo kao

$$a_{18}a_{17}a_{16} \quad a_{15}a_{14}a_{13}a_{12}a_{11}a_{10}a_9a_8 \quad a_7a_6a_5a_4a_3a_2a_1a_0,$$

gdje s razmakom odvajamo riječi. Konkretan primjer bi bio

$$\theta^{18} + \theta^{15} + \theta^{12} + \theta^9 + \theta^6 + \theta^5 + \theta^3 + \theta + 1$$

odnosno pomoću bitova kao

$$100 \quad 10010010 \quad 01101011.$$

Prva riječ nije cijela iskorištena (jer n nije višekratnik od w). Neiskorištene bitove možemo popuniti nulama (ali nije nužno) pa na kraju dobijemo

$$00000100 \quad 10010010 \quad 01101011.$$

Možemo promatrati i proširena polja s karakteristikom 3. Element od $\mathbb{F}_{3^n}$ je reprezentiran polinomom stupnja $\leqslant n-1$ s koeficijentima iz skupa $\{0,1,2\}$. Kako sada imamo tri mogućnosti za koeficijent, a kod polja sa karakteristikom 2 smo imali dva, treba nam pametan način za prikaz tih brojeva pomoću bitova. Jedna mogućnost je koristiti par bitova. Koeficijente $0,1,2$ ćemo kodirati sa $11,01,10$ (kao i Kawahara, Aoki, Tagaki [3]) za aritmetiku nad $\mathbb{F}_{3^n}$.

Dakle, element

$$a_{n-1}\theta^{n-1} + a_{n-2}\theta^{n-2} + \cdots + a_1\theta + a_0$$

gdje je $a_i \in \{0,1,2\}$, će biti reprezentiran nizom $h_{n-1}l_{n-1}h_{n-2}l_{n-2}\ldots h_1l_1h_0l_0$ duljine $2n$, gdje par bitova h_il_i predstavlja a_i. Radi preglednijeg zapisa imat ćemo dva niza $h_{n-1}h_{n-2}\ldots h_1h_0$ i $l_{n-1}l_{n-2}\ldots l_1l_0$ svaki veličine n. Svaki od njih ćemo zapisivati pomoću riječi duljine w, kao i kod $\mathbb{F}_{2^n}$.

Primjer 4.1.2. *Promatramo $\mathbb{F}_{3^{19}}$ kao $\mathbb{F}_3(\theta)$, gdje je θ korijen od $f(x) = x^{19}+x^2+2$. Uzmimo element*

$$\theta^{18} + 2\theta^{16} + 2\theta^{15} + \theta^{13} + \theta^{10} + 2\theta^8 + \theta^6 + 2\theta^5 + \theta^3 + 2\theta$$

iz $\mathbb{F}_{3^{19}}$. Ovaj polinom ćemo reprezentirati kao 1022010010201201020*. Neka nam je riječ opet veličine $w = 8$ bita, imamo*

High-order bit array	011	11011011	10110111
Low-order bit array	110	01111110	11011101

i opet smo s razmakom razdvojili pojedine riječi.

4.2 Zbrajanje i oduzimanje

Ponovo ćemo promatrati proširena polja karakteristike 2 i 3. U polju karakteristike 2 zbrajanje nam je jednostavna XOR operacija nad bitovima. Ono što nam povećava efikasnost je činjenica da imamo riječi veličine 8 bitova pa možemo raditi XOR nad cijelom riječi.

Primjer 4.2.1. *Uzmimo ponovo prošireno polje $\mathbb{F}_{2^{19}}$ i sljedeća dva elementa*

$\theta^{17}+\theta^{16}+\theta^{15}+\theta^{12}+\theta^{11}+\theta^9+\theta^7+\theta^5+\theta^3+\theta$	011	10011010	10101010
$\theta^{18}+\theta^{16}+\theta^{14}+\theta^{13}+\theta^{11}+\theta^7+\theta^6+\theta^5+\theta^4+1$	101	01101000	11110001.

Operacija XOR nad ova dva niza bitova nam daje

$$110 \quad 11110010 \quad 01011011.$$

Odnosno

$$\theta^{18} + \theta^{17} + \theta^{15} + \theta^{14} + \theta^{13} + \theta^{12} + \theta^9 + \theta^6 + \theta^4 + \theta^3 + \theta + 1$$

što je očito suma početna dva elementa modulo 2.

Zbrajanje u poljima karakteristike 3 je ipak malo složenije. Koeficijente $0, 1, 2$ ćemo kodirati sa $11, 01, 10$ kao i u prijašnjem poglavlju te ćemo opet organizirati nizove u riječi od $w = 8$ bitova. Na ulazu ćemo imati α i β, odnosno α kao α_h i α_l te β_h i β_l za β. Rezultat zbrajanja $\gamma = \alpha + \beta$ će nam opet biti dva niza γ_h i γ_l.

$$\gamma_h = (\alpha_l \text{XOR} \beta_l) \text{ OR } ((\alpha_h \text{XOR} \beta_h) \text{ XOR} \alpha_l)$$
$$\gamma_l = (\alpha_h \text{XOR} \beta_h) \text{ OR } ((\alpha_l \text{XOR} \beta_l) \text{ XOR} \alpha_h)$$

Primjer 4.2.2. *Uzmimo prošireno polje $\mathbb{F}_{3^{19}}$ te α i β te izračunajmo α_h, α_l, β_h i β_l.*

α	=	$2\theta^{17} + \theta^{15} + \theta^{12} + 2\theta^9 + \theta^8 + 2\theta^7 + \theta^5 + \theta^3 + 2\theta^2 + \theta$		
α_h	:	111	01101110	11010101
α_l	:	101	11111101	01111011
β	=	$\theta^{18} + 2\theta^{15} + \theta^{13} + 2\theta^{10} + \theta^8 + \theta^5 + 2\theta^4 + \theta^3 + \theta^2 + 1$		
β_h	:	011	11011110	11010010
β_l	:	111	01111011	11101111

Trebaju nam pomoćni nizovi $\tau_1, \tau_2, \tau_3, \tau_4$ za izračunavanje γ_h i γ_l.

τ_1	=	α_h XOR β_h	=	100	10110000	00000111
τ_2	=	α_l XOR β_l	=	010	10000110	10010100
τ_3	=	τ_1 XOR α_l	=	001	01001101	01111100
τ_4	=	τ_2 XOR α_h	=	101	11101000	01000001
γ_h	=	τ_2 OR τ_3	=	011	11001111	11111100
γ_l	=	τ_1 OR τ_4	=	101	11111000	01000111

γ je 1200011022220222011*, odnosno sljedeći polinom je očito $(\alpha + \beta)$ modulo 3*

$$\theta^{18} + 2\theta^{17} + \theta^{13} + \theta^{12} + 2\theta^{10} + 2\theta^9 + 2\theta^8 + 2\theta^7 + 2\theta^5 + 2\theta^4 + 2\theta^3 + \theta + 1.$$

Oduzimanje u $\mathbb{F}_{3^n}$ vrijedi $\alpha - \beta = \alpha + (-\beta)$, a $-\beta$ dobijemo iz β zamjenom β_h i β_l.

4.3 Množenje

Množenje u $\mathbb{F}_{p^n}$ zahtjeva dvije operacije. Prvo pomnožimo faktore kao polinome u $\mathbb{F}_p[x]$ i dobijemo rezultat koji je stupnja $\leqslant 2(n-1)$. Nakon toga taj rezultat podijelimo definirajućim polinomom $f(x)$. Ostatak (polinom stupnja manjeg od n) je kanonski predstavnik umnoška u polju. U nastavku ćemo promatrati samo polja karakteristike 2.

Neka imamo dva polinoma a i b stupnja manjeg od n. Prvo inicijaliziramo produkt kao polinom stupnja $2(n-1)$. Za svaki koeficijent $b_i \neq 0$ iz $b_i x^i$ ćemo pomnožiti a sa b_i te pomaknuti za i mjesta u lijevo i dodati produktu. Za naše polje karakteristike 2 jedina vrijednost od b_i koja nije 0 je 1 pa moramo samo pomicati i dodavati (XOR).

Primjer 4.3.1. *Ponovo ćemo koristiti iste α i β kao i prije.*

$$\alpha = \theta^{17} + \theta^{16} + \theta^{15} + \theta^{12} + \theta^{11} + \theta^9 + \theta^7 + \theta^5 + \theta^3 + \theta = 011 \quad 10011010 \quad 10101010$$
$$\beta = \theta^{18} + \theta^{16} + \theta^{14} + \theta^{13} + \theta^{11} + \theta^7 + \theta^6 + \theta^5 + \theta^4 + 1 = 101 \quad 01101000 \quad 11110001$$

U tablici možemo vidjeti eksponente i od β gdje je $b_i \neq 0$ koji nam govore koliko ćemo pomaknuti u lijevo te polinom α. Na kraju napravimo XOR nad riječima i dobijemo traženi rezultat, odnosno umnožak α i β.

i			$x^i\alpha(x)$		
0			011	10011010	10101010
4			0111001	10101010	1010
5			01110011	01010101	010
6		0	11100110	10101010	10
7		01	11001101	01010101	0
11		011100	11010101	01010	
13		01110011	01010101	010	
14	0	11100110	10101010	10	
16	011	10011010	10101010		
18	01110	01101010	101010		
	01101	01111000	01001010	00001010	11001010

Navedeni algoritam za množenje se može ubrzati, proći ćemo kroz ubrzanje za polja karakteristike 2, ali analogno je i za polja karakteristike 3.

4.4 Češalj metode

Slijeva nadesno

Češalj metoda slijeva nadesno pomiče polinom produkta (umjesto prvog faktora). Ova metoda obrađuje pozicije bitova $j = w-1, w-2, \ldots, 1, 0$ u riječi, u tom redoslijedu. Za sve riječi u β s postavljenim j-tim bitom, α se dodaje produktu s odgovarajućim pomacima na razini riječi. Kada se određeni j obrađuje, produkt se množi s x (pomaknut ulijevo za jedan bit), tako da je poravnat na slijedeću $(j-1)$-u poziciju bita u riječi.

Primjer 4.4.1. *Ovu metodu ćemo primjeniti na primjer 4.3.1. Produkt γ ćemo inicijalizirati na nulu kao polinom stupnja 36 i j−ta riječ od γ je označena kao γ_j.*

		$\alpha =$			011	10011010	10101010
		$x^8\alpha =$		011	10011010	10101010	
		$x^{16}\alpha =$	011	10011010	10101010		
j	i	operacija	γ				
			γ_4	γ_3	γ_2	γ_1	γ_0
		inicijalizacija γ	00000	00000000	00000000	00000000	00000000
7	7	α XOR γ	00000	00000000	00000011	10011010	10101010
		γ pomak u lijevo γ	00000	00000000	00000111	00110101	01010100
6	6	α XOR γ	00000	00000000	00000100	10101111	11111110
	14	$x^8\alpha$ XOR γ	00000	00000011	10011110	00000101	11111110
		γ pomak u lijevo	00000	00000111	00111100	00001011	11111100
5	5	α XOR γ	00000	00000111	00111111	10010001	01010110
	13	$x^8\alpha$ XOR γ	00000	00000100	10100101	00111011	01010110
		γ pomak u lijevo	00000	00001001	01001010	01110110	10101100
4	4	α XOR γ	00000	00001001	01001001	11101100	00000110
		γ pomak u lijevo	00000	00010010	10010011	11011000	00001100
3	11	$x^8\alpha$ XOR γ	00000	00010001	00001001	01110010	00001100
		γ pomak u lijevo	00000	00100010	00010010	11100100	00011000
2	18	$x^{16}\alpha$ XOR γ	00011	10111000	10111000	11100100	00011000
		γ pomak u lijevo	00111	01110001	01110001	11001000	00110000
1		γ pomak u lijevo	01110	11100010	11100011	10010000	01100000
0	0	α XOR γ	01110	11100010	11100000	00001010	11001010
	16	$x^{16}\alpha$ XOR γ	01101	01111000	01001010	00001010	11001010

Možemo vidjeti da smo dobili isti rezultat kao i u primjeru 4.3.1.

Zdesna nalijevo

Ono što možemo primjetiti u algoritmu za množenje 4.3 je da se pomaci $x^j\alpha(x)$ i $x^j\alpha(x)$ razlikuju samo po pratećim praznim (0) riječima ako $i \equiv j \pmod{w}$. Dakle, pomaknute polinome $x^j\alpha(x)$ treba izračunati samo za $j = 0, 1, 2, \ldots, w-1$. Nakon što se izračuna pomaknuta vrijednost $x^j\alpha(x)$, ona se može koristiti za sve koeficijente koji nisu nula $b_i = 1$ s $i = j + kw$ za $k = 0, 1, 2, \ldots$. Sve što trebamo je dodati $x^j\alpha(x)$ počevši od k-te riječi (s desna) produkta. Ova metoda se naziva *češalj metoda zdesna nalijevo*.

Primjer 4.4.2. *Ako primjenimo tu metodu na primjer 4.3.1 moramo izračunati $x^j\alpha(x)$ samo za $j = 0, 1, 2, \ldots, 7$. Imamo $x^0\alpha(x) = \alpha(x)$ i vrijedi $x^j\alpha(x) = x \times \left(x^{j-1}\alpha(x)\right)$ za $j = 1, 2, \ldots, 7$, a $x^j\alpha(x)$ dobijemo iz $x^{j-1}\alpha(x)$ pomicanjem ulijevo. Znači, možemo iskoristiti $x^0\alpha(x)$ za $i = 0, 16$, $x^1\alpha(x)$ nam ne treba, $x^2\alpha(x)$ za $i = 18$, $x^3\alpha(x)$ za $i = 11$, $x^4\alpha(x)$ za $i = 4$, $x^5\alpha(x)$ za $i = 5, 13$, $x^6\alpha(x)$ za $i = 6, 14$ i $x^7\alpha(x)$ za $i = 7$.*

Ubrzanje češalj metoda

Osnovna ideja je koristiti prozor neke veličine k. Produkte $\alpha\delta$ izračunamo unaprijed i zapišemo za svih 2^k polinoma δ stupnja manjeg od k. U petlji množenja, k bitova od β se obrađuje odjednom. Umjesto dodavanja α (ili pomaknute verzije α) za svaki jedan bit od β, dodajemo unaprijed izračunati polinom $\alpha\delta$ (ili njegovu prikladno pomaknutu verziju), gdje δ predstavlja k-bitni dio koji se čita iz drugog polinoma β. Uglavnom je $k = 4$.

Primjer 4.4.3. *Pogledajmo kako primjeniti ovo ubrzanje na metodu zdesna nalijevo. Uzet ćemo već poznate α i β te $k = 2$.*

$$\alpha = \theta^{17} + \theta^{16} + \theta^{15} + \theta^{12} + \theta^{11} + \theta^9 + \theta^7 + \theta^5 + \theta^3 + \theta = 011 \quad 10011010 \quad 10101010$$
$$\beta = \theta^{18} + \theta^{16} + \theta^{14} + \theta^{13} + \theta^{11} + \theta^7 + \theta^6 + \theta^5 + \theta^4 + 1 = 101 \quad 01101000 \quad 11110001$$

Slijede četiri produkta koje izračunamo unaprijed i kasnije iskoristimo.

$$\begin{array}{lcllll}
(00)\alpha(x) & = & (0x+0)\alpha(x) & = & 0000 & 00000000 \quad 00000000 \\
(01)\alpha(x) & = & (0x+1)\alpha(x) & = & 0011 & 10011010 \quad 10101010 \\
(10)\alpha(x) & = & (1x+0)\alpha(x) & = & 0111 & 00110101 \quad 01010100 \\
(11)\alpha(x) & = & (1x+1)\alpha(x) & = & 0100 & 10101111 \quad 11111110
\end{array}$$

i	bitovi $b_{i+1}b_i$ iz β	$x^i(b_{i+1}x + b_i)\alpha$				
0	01			0011	10011010	10101010
2	00					
4	11			01001010	11111111	1110
6	11		01	00101011	11111111	10
8	00					
10	10		011100	11010101	010100	
12	10		01110011	01010101	0100	
14	01	00	11100110	10101010	10	
16	01	0011	10011010	10101010		
18	01	001110	01101010	101010		
		001101	01111000	01001010	00001010	11001010

Primjer 4.4.4. *Ubrzanje metode slijeva nadesno.*

j	i	$b_{i+1}b_i$		vrijednost					oper
			$\gamma =$	00000	00000000	00000000	00000000	00000000	inic
6	6	11	$(11)\alpha =$			0100	10101111	11111110	
			$\gamma =$	00000	00000000	00000100	10101111	11111110	XOR
	14	01	$x^8(01)\alpha =$		0011	10011010	10101010		
			$\gamma =$	00000	00000011	10011110	00000101	11111110	XOR
			$\gamma =$	00000	00001110	01111000	00010111	11111000	lpom
4	4	11	$(11)\alpha =$			0100	10101111	11111110	
			$\gamma =$	00000	00001110	01111100	10111000	00000110	XOR
	12	10	$x^8(10)\alpha =$		0111	00110101	01010100		
			$\gamma =$	00000	00001001	01001001	11101100	00000110	XOR
			$\gamma =$	00000	00100101	00100111	10110000	00011000	lpom
2	2	00							
	10	10	$x^8(10)\alpha =$		0111	00110101	01010100		
			$\gamma =$	00000	00100010	00010010	11100100	00011000	XOR
	18	01	$x^{16}(01)\alpha =$	0011	10011010	10101010			
			$\gamma =$	00011	10111000	10111000	11100100	00011000	XOR
			$\gamma =$	01110	11100010	11100011	10010000	01100000	lpom
0	0	01	$(01)\alpha =$			0011	10011010	10101010	
			$\gamma =$	01110	11100010	11100000	00001010	11001010	XOR
	8	00							
	16	01	$x^{16}(01)\alpha =$	0011	10011010	10101010			
			$\gamma =$	01101	01111000	01001010	00001010	11001010	XOR

4.5 Modularna redukcija

Pretpostavljamo da imamo polinom $\gamma(x)$ stupnja $\leqslant 2(n-1)$. Naš zadatak je izračunati ostatak $\rho(x) = \gamma(x) \operatorname{rem} {}^{1} f(x)$, gdje je $\deg f(x) = n$. Euklidsko dijeljenje polinoma nastavlja uklanjati članove stupnjeva većih od n oduzimanjem odgovarajućih višekratnika $f(x)$ od $\gamma(x)$. Prirodno je ukloniti članove različite od nule jedan po jedan iz $\gamma(x)$ u padajućem redoslijedu njihovih stupnjeva. Oduzimanje višekratnika od $f(x)$ može uvesti nove članove različite od nule, tako da općenito nije jednostavno eliminirati više članova različitih od nule istovremeno. Za polinome nad $\mathbb{F}_2$, jedini koeficijent koji nije nula je 1. Kako bismo uklonili član koji nije nula x^i od $\gamma(x)$, moramo oduzeti (ili XOR) $x^{i-n} f(x)$ od $\gamma(x)$, gdje se $x^{i-n} f(x)$ može učinkovito izračunati pomakom $f(x)$ ulijevo za $i-n$ bitova. Na kraju se $\gamma(x)$ svodi na polinom stupnja manjeg od n. Ovo je željeni ostatak $\rho(x)$.

Primjer 4.5.1. *Uzmimo rezultat iz prošlog primjera i reducirajmo ga ovom metodom.*

Dobili smo da produkt α i β iz primjera 4.3.1 u $\mathbb{F}_{2^{19}}$ iznosi $\theta^{17} + \theta^{16} + \theta^{15} + \theta^{13} + \theta^{10} + \theta^9 + \theta^2 + \theta + 1$.

Modularna redukcija može biti učinkovitija ako je definirajući polinom $f(x)$ odabran na odgovarajući način. Prvo, želimo da $f(x)$ ima što manje članova različitih od nule (ireducibilni binomi, trinomi, kvadrinomi i pentanomi). Drugo, stupnjevi članova različitih od nule u $f(x)$ (osim samog x^n) trebaju biti što niži. Drugim riječima, najveći stupanj n_1 ovih članova trebao bi biti dovoljno manji od n. Ako $n - n_1 \geqslant w$ (gdje je w veličina riječi), poništavanje člana koji nije nula ax^i oduzimanjem $ax^{i-n} f(x)$ iz $\gamma(x)$ ne utječe na druge koeficijente koji se nalaze u istoj riječi od $\gamma(x)$ pohranjujući koeficijent od x^i. To znači da sada možemo poništiti cijelu riječ zajedno.

Da budemo precizniji, usredotočimo se na binarna polja i napišimo $f(x) = x^n + f_1(x)$ s $n_1 = \deg f_1(x) \leqslant n - w$. Želimo poništiti krajnju lijevu riječ koja nije nula μ iz $\gamma(x)$. Jasno je da je μ polinom stupnja $\leqslant w - 1$. Ako je μ r-ta riječ u γ, trebamo dodati (XOR) $x^{rw-n}\mu f(x)$ u $\gamma(x)$. Ali $x^{rw-n}\mu f(x) = x^{rw}\mu + x^{rw-n}\mu f_1(x)$. Prvi dio $x^{rw}\mu$ je upravo r-ta riječ od γ, tako da ovu riječ možemo postaviti na nulu bez stvarnog izvođenja zbrajanja. Uvjet $n_1 \leqslant n-w$ označava da drugi dio $x^{rw-n}\mu f_1(x)$ nema članove različite od nule u r-toj riječi od γ. Budući da je množenje s x^{rw-n} pomak ulijevo, jedini netrivijalni izračun je onaj za $\mu f_1(x)$, ali μ ima mali stupanj ($\leqslant w-1$). Ako i $f_1(x)$ ima samo nekoliko članova koji nisu nula, ovo množenje može biti prilično učinkovito. Za ovo množenje možemo koristiti češalj metodu kako bismo postigli veću učinkovitost. Budući da je $f_1(x)$ polinom ovisan o reprezentaciji polja (ali ne i o operandima), predračun za češalj metodu s prozorom potrebno je izvršiti samo jednom, za sve redukcijske operacije u polju. Čak i osmobitni prozori mogu biti izvedivi u smislu pohrane ako $f_1(x)$ ima samo nekoliko koeficijenata koji nisu nula.

[1] rem je ostatak pri dijeljenju

i		vrijednost					oper
	$\gamma(x) =$	01101	01111000	01001010	00001010	11001010	inic
35	$x^{16}f(x) =$	1000	00000000	00100111			lpom
	$\gamma(x) =$	00101	01111000	01101101	00001010	11001010	XOR
34	$x^{15}f(x) =$	100	00000000	00010011	1		lpom
	$\gamma(x) =$	00001	01111000	01111110	10001010	11001010	XOR
32	$x^{13}f(x) =$	1	00000000	00000100	111		lpom
	$\gamma(x) =$	00000	01111000	01111010	01101010	11001010	XOR
30	$x^{11}f(x) =$		1000000	00000001	00111		lpom
	$\gamma(x) =$	00000	00111000	01111011	01010010	11001010	XOR
29	$x^{10}f(x) =$		100000	00000000	100111		lpom
	$\gamma(x) =$	00000	00011000	01111011	11001110	11001010	XOR
28	$x^{9}f(x) =$		10000	00000000	0100111		lpom
	$\gamma(x) =$	00000	00001000	01111011	10000000	11001010	XOR
27	$x^{8}f(x) =$		1000	00000000	00100111		lpom
	$\gamma(x) =$	00000	00000000	01111011	10100111	11001010	XOR
22	$x^{3}f(x) =$			1000000	00000001	00111	lpom
	$\gamma(x) =$	00000	00000000	00111011	10100110	11110010	XOR
21	$x^{2}f(x) =$			100000	00000000	100111	lpom
	$\gamma(x) =$	00000	00000000	00011011	10100110	01101110	XOR
20	$x^{1}f(x) =$			10000	00000000	0100111	lpom
	$\gamma(x) =$	00000	00000000	00001011	10100110	00100000	XOR
19	$x^{0}f(x) =$			1000	00000000	00100111	lpom
	$\gamma(x) =$	00000	00000000	00000011	10100110	00000111	XOR

Poglavlje 5

Algoritmi od interesa za primjene u kriptografiji

Uzmimo element α u polju, različit od nule. Moramo izračunati element polja u tako da je $u\alpha = 1$. Svi algoritmi u ovom poglavlju izračunavaju prošireni NZD od α s definirajućim polinomom f. Budući da je f ireducibilan, a α nije nula sa stupnjem manjim od $n = \deg f$, imamo $\mathrm{NZD}(\alpha, f) = 1 = u\alpha + vf$ za neke polinome u, v. Zanima nas računanje u. α i f su dva ulazna parametra za NZD algoritme. Uzimamo u obzir samo binarna polja $\mathbb{F}_{2^n}$, pri čemu su prilagodbe na druga polja $\mathbb{F}_{p^n}$ prilično jednostavne.

5.1 Euklidov inverz

Poput cijelih brojeva, Euklidov NZD algoritam generira niz ostataka inicijaliziran sa $r_0 = f$ i $r_1 = \alpha$. Nakon toga, za $i = 2, 3, \ldots$, izračunava se $r_i = r_{i-2}$ rem r_{i-1}. Održavamo dva druga niza u_i i v_i koji zadovoljavaju $u_i\alpha + v_i f = r_i$ za sve $i \geqslant 0$. Inicijaliziramo $u_0 = 0, u_1 = 1, v_0 = 1, v_1 = 0$ tako da je jednakost zadovoljena za $i = 0, 1$. Ako je $q_i = r_{i-2}$ quot [1] r_{i-1}, tada se r_i može napisati kao $r_i = r_{i-2} - q_i r_{i-1}$. Analogno ažuriramo i u i v nizove, odnosno, $u_i = u_{i-2} - q_i u_{i-1}$ i $v_i = v_{i-2} - q_i v_{i-1}$. Lako se može provjeriti da ove nove vrijednosti i dalje zadovoljavaju $u_i\alpha + v_i f = r_i$.

Za inverz nije potrebno eksplicitno izračunati niz v. Čak i ako je v_i potrebno na kraju NZD petlje, to možemo dobiti kao $v_i = (r_i - u_i\alpha)/f$. Budući da svaki r_i i svaki u_i ovise o samo dva prethodna izraza, moramo čuvati podatke samo iz dvije prethodne iteracije.

Primjer 5.1.1. *Definirajmo $\mathbb{F}_{2^7}$ ireducibilnim polinomom $f(x) = x^7 + x^3 + 1$ i izračunajmo inverz od $\alpha(x) = x^6 + x^4 + x^2$, odnosno $\alpha = \theta^6 + \theta^4 + \theta^2$, gdje je θ korijen od f. Koristimo x umjesto θ kako bismo naglasili da radimo u $\mathbb{F}_2[x]$.*

[1] quot je kvocijent pri dijeljenju

i	q_i	r_i	u_i
0		$x^7 + x^3 + 1$	0
1		$x^6 + x^4 + x^2$	1
2	x	$x^5 + 1$	x
3	x	$x^4 + x^2 + x$	$x^2 + 1$
4	x	$x^3 + x^2 + 1$	x^3
5	$x + 1$	1	$x^4 + x^3 + x^2 + 1$

Slijedi da je $\alpha^{-1} = x^4 + x^3 + x^2 + 1$, *odnosno* $\alpha^{-1} = \theta^4 + \theta^3 + \theta^2 + 1$.

5.2 Binarni inverz

Binarni inverz u $\mathbb{F}_{2^n}$ izravna je prilagodba proširenog binarnog NZD algoritma za cijele brojeve. Algoritam 1 opisuje binarni inverz. Dva polinoma $\alpha(x)$ i $f(x)$ su ulazni podaci. Algoritam 1 održava jednakosti

$$u_1\alpha + v_1 f = r_1,$$
$$u_2\alpha + v_2 f = r_2.$$

Ovdje se r_1, r_2 ponašaju kao niz ostataka Euklidovog NZD. Ostali nizovi u i v podliježu istim transformacijama kao i niz r. Ne održavamo eksplicitno v niz. Ovaj niz je neophodan samo za razumijevanje ispravnosti algoritma.

Problem je sada u tome što kada prisilimo r_1 (ili r_2) da bude djeljiv s x, polinom u_1 (ili u_2) ne mora biti djeljiv s x. Ipak, moramo izdvojiti x iz u_1 (ili u_2). To se postiže međusobnim podešavanjem vrijednosti u i v. Pretpostavimo $x \mid r_1$, ali $x \nmid u_1$ i želimo poništiti x iz $u_1\alpha + v_1 f = r_1$. Budući da $x \nmid u_1$, konstantni član u u_1 mora biti 1. Nadalje, budući da je f ireducibilan polinom, njegov konstantni član također mora biti 1. Ali tada konstantni član u $u_1 + f$ je nula, odnosno vrijedi $x \mid (u_1 + f)$. Formulu jednakosti zapisujemo kao $(u_1 + f)\,\alpha + (v_1 + \alpha)\,f = r_1$. Budući da x dijeli i r_1 i $u_1 + f$ (ali ne i f), x također mora dijeliti $v_1 + \alpha$. Dakle, sada možemo poništiti x u cijeloj jednadžbi.

Algorithm 1 Binarni inverz

Initialize: $r_1 = \alpha$, $r_2 = f$, $u_1 = 1$, $u_2 = 0$
  repeat
    while $(r_1 \mid x)$ **do**
      $r_1 = r_1/x$
      if $(u_1 \nmid x)$ **then**
        $u_1 = u_1 + f$
      $u_1 = u_1/x$
      if $(r_1 = 1)$ **then**
        return u_1
    while $(r_2 \mid x)$ **do**
      $r_2 = r_2/x$
      if $(u_2 \nmid x)$ **then**
        $u_2 = u_2 + f$
      $u_2 = u_2/x$
      if $(r_2 = 1)$ **then**
        return u_2
    if $(\deg r_1 \geqslant \deg r_2)$ **then**
      $r_1 = r_1 + r_2$
      $u_1 = u_1 + u_2$
    else
      $r_2 = r_2 + r_1$
      $u_2 = u_2 + u_1$
  until $r_1 = 1$ **or** $r_2 = 1$

Primjer 5.2.1. *Uzimamo $\mathbb{F}_{2^7}$ i ireducibilni polinom $f(x) = x^7 + x^3 + 1$, izračunavamo α^{-1}, gdje je $\alpha(x) = x^6 + x^4 + x^2$.*

r_1	r_2	u_1	u_2
$x^6 + x^4 + x^2$	$x^7 + x^3 + 1$	1	0
dijeli r_1 sa x dok možeš i podesi u_1			
$x^5 + x^3 + x$	$x^7 + x^3 + 1$	$x^6 + x^2$	0
$x^4 + x^2 + 1$	$x^7 + x^3 + 1$	$x^5 + x$	0
postavi $r_2 = r_2 + r_1$ i $u_2 = u_2 + u_1$			
$x^4 + x^2 + 1$	$x^7 + x^4 + x^3 + x^2$	$x^5 + x$	$x^5 + x$
dijeli r_2 sa x dok možeš i podesi u_2			
$x^4 + x^2 + 1$	$x^6 + x^3 + x^2 + x$	$x^5 + x$	$x^4 + 1$
$x^4 + x^2 + 1$	$x^5 + x^2 + x + 1$	$x^5 + x$	$x^6 + x^3 + x^2$
postavi $r_2 = r_2 + r_1$ i $u_2 = u_2 + u_1$			
$x^4 + x^2 + 1$	$x^5 + x^4 + x$	$x^5 + x$	$x^6 + x^5 + x^3 + x^2 + x$
dijeli r_2 sa x dok možeš i podesi u_2			
$x^4 + x^2 + 1$	$x^4 + x^3 + 1$	$x^5 + x$	$x^5 + x^4 + x^2 + x + 1$
postavi $r_1 = r_1 + r_2$ i $u_1 = u_1 + u_2$			
$x^3 + x^2$	$x^4 + x^3 + 1$	$x^4 + x^2 + 1$	$x^5 + x^4 + x^2 + x + 1$
dijeli r_1 sa x dok možeš i podesi u_1			
$x^2 + x$	$x^4 + x^3 + 1$	$x^6 + x^3 + x^2 + x$	$x^5 + x^4 + x^2 + x + 1$
$x + 1$	$x^4 + x^3 + 1$	$x^5 + x^2 + x + 1$	$x^5 + x^4 + x^2 + x + 1$
postavi $r_2 = r_2 + r_1$ i $u_2 = u_2 + u_1$			
$x + 1$	$x^4 + x^3 + x$	$x^5 + x^2 + x + 1$	x^4
dijeli r_2 sa x dok možeš i podesi u_2			
$x + 1$	$x^3 + x^2 + 1$	$x^5 + x^2 + x + 1$	x^3
postavi $r_2 = r_2 + r_1$ i $u_2 = u_2 + u_1$			
$x + 1$	$x^3 + x^2 + x$	$x^5 + x^2 + x + 1$	$x^5 + x^3 + x^2 + x + 1$
dijeli r_2 sa x dok možeš i podesi u_2			
$x + 1$	$x^2 + x + 1$	$x^5 + x^2 + x + 1$	$x^6 + x^4 + x + 1$
postavi $r_2 = r_2 + r_1$ i $u_2 = u_2 + u_1$			
$x + 1$	x^2	$x^5 + x^2 + x + 1$	$x^6 + x^5 + x^4 + x^2$
dijeli r_2 sa x dok možeš i podesi u_2			
$x + 1$	x	$x^5 + x^2 + x + 1$	$x^5 + x^4 + x^3 + x$
$x + 1$	1	$x^5 + x^2 + x + 1$	$x^4 + x^3 + x^2 + 1$

Kako nam je $r_2 = 1$, $\alpha^{-1} = u_2 = x^4 + x^3 + x^2 + 1$.

Za cijele brojeve, binarni NZD je obično brži od Euklidovog NZD, budući da je Euklidovo dijeljenje znatno skuplje od zbrajanja i pomaka. Za polinome, binarni inverz i Euklidov inverz imaju usporedive performanse. Euklidov inverz može promatrati kao niz uklanjanja najznačajnijih članova iz jednog od ostataka. U binarnom inverzu, član se uklanja s najmanje značajnog kraja, a naknadno dijeljenje s x vraća najmanje značajan član natrag na 1. Oba ova procesa uklanjanja koriste približno isti broj i vrste (pomak i XOR) operacija.

5.3 Gotovo inverz

Gotovo inverz algoritam je varijanta binarnog inverza. U binarnom inverzu poništavamo x iz r_1 i u_1 (ili iz r_2 i u_2) unutar NZD petlje. Proces uključuje uvjetno dodavanje f u u_1 (ili u_2). U gotovo inverzu, ne mičemo x iz u (i v) nizova (ali pamtimo koliko x treba maknuti). Nakon što petlja završi, maknemo sve te x iz u_1 ili u_2. Točnije, sada održavamo invarijantnosti

$$u_1\alpha + v_1 f = x^k r_1,$$
$$u_2\alpha + v_2 f = x^k r_2,$$

za neki cijeli broj $k \geqslant 0$. Vrijednost k se mijenja s vremenom (i treba je zapamtiti), ali mora biti ista u obje jednadžbe u istom trenutku. Pretpostavimo da i r_1 i r_2 imaju konstantne članove 1 i $\deg r_1 \geqslant \deg r_2$. U tom slučaju dodajemo drugu jednadžbu prvoj da bismo dobili

$$(u_1 + u_2)\,\alpha + (v_1 + v_2)\,f = x^k\,(r_1 + r_2)\,.$$

Preimenovanje u_1+u_2 u u_1, v_1+v_2 u v_1 i r_1+r_2 u r_1 daje $u_1\alpha+v_1 f = x^k r_1$. Sada je r_1 djeljivo s x. Neka je t najveći eksponent za koji x^t dijeli r_1. Maknemo x^t iz r_1 i preimenujemo r_1/x^t u r_1 da dobijemo

$$u_1\alpha + v_1 f = x^{k+t} r_1.$$

Ovdje ne ažuriramo u_1 i v_1. Međutim, budući da se vrijednost k promijenila u $k + t$, druga se jednadžba mora ažurirati kako bi bila u skladu s tim, to jest, druga se jednadžba transformira kao

$$(x^t u_2)\,\alpha + (x^t v_2)\,f = x^{k+t} r_2.$$

Preimenovanje $x^t u_2$ u u_2 i $x^t v_2$ u v_2 vraća obje invarijantnosti. Algoritam 2 implementira ovu ideju. Ne trebamo eksplicitno održavati v_1, v_2.

Algorithm 2 Gotovo inverz

Initialize: $r_1 = \alpha$, $r_2 = f$, $u_1 = 1$, $u_2 = 0$, $k = 0$
  repeat
    if $(r_1 \mid x)$ **then**
      Let $x^t \mid r_1$ but $x^{t+1} \nmid r_1$
      $r_1 = r_1/x^t$
      $u_2 = x^t u_2$
      $k = k + t$
      if $(r_1 = 1)$ **then**
        return $x^{-k}u_1 \pmod f$
    if $(r_2 \mid x)$ **then**
      Let $x^t \mid r_2$ but $x^{t+1} \nmid r_2$
      $r_2 = r_2/x^t$
      $u_1 = x^t u_1$
      $k = k + t$
      if $(r_2 = 1)$ **then**
        return $x^{-k}u_2 \pmod f$
    if $(\deg r_1 \geqslant \deg r_2)$ **then**
      $r_1 = r_1 + r_2$
      $u_1 = u_1 + u_2$
    else
      $r_2 = r_2 + r_1$
      $u_2 = u_2 + u_1$
  until $r_1 = 1$ **or** $r_2 = 1$

Moramo maknuti potreban broj x-eva nakon završetka petlje. Pretpostavimo da petlja završava zbog uvjeta $r_1 = 1$. U tom slučaju imamo $u_1\alpha + v_1 f = x^k$ za neki k. Ali onda, $\alpha^{-1} = x^{-k}u_1$ modulo f. Isto tako, ako r_2 postane 1, trebamo izračunati $x^{-k}u_2$ modulo f. Pretpostavimo da $x^{-k}u$ treba izračunati modulo f za neki u. Jedna je mogućnost dijeliti u s x što je dulje moguće. Kada konstantni član u u postane 1, f mu se dodaje i proces se nastavlja sve dok se x ne ukloni k puta. To znači izvođenje istih izračuna kao u algoritmu 1 (iako na drugom mjestu u algoritmu).

Ako je f nekog posebnog oblika, postupak uklanjanja može biti donekle učinkovit. Pretpostavimo da je x^l član različit od nule u f s najmanjim stupnjem > 0. Neka h označava zbroj članova koji nisu nula od u sa stupnjevima $< l$ (članovi koji uključuju $x^0, x^1, \ldots, x^{l-1}$). Budući da je $u + hf$ djeljiv s x^l, l pojavljivanja x može se istovremeno ukloniti iz $u + hf$. Za male l ($l = 1$ u najgorem slučaju), uklanjanje x zahtjeva previše ponavljanja. Ako l nije premalen, mnogo x-ova se uklanja po iteraciji i očekujemo da će gotovo inverz raditi malo učinkovitije od binarnog inverza.

Primjer 5.3.1. *Uzimamo* $\mathbb{F}_{2^7}$, $f(x) = x^7 + x^3 + 1$ *i* $\alpha(x) = x^6 + x^4 + x^2$.

r_1	r_2	u_1	u_2	t
$x^6 + x^4 + x^2$	$x^7 + x^3 + 1$	1	0	0
dijeli r_1 sa x^2 i podesi u_2				
$x^4 + x^2 + 1$	$x^7 + x^3 + 1$	1	0	2
postavi $r_2 = r_2 + r_1$ i $u_2 = u_2 + u_1$				
$x^4 + x^2 + 1$	$x^7 + x^4 + x^3 + x^2$	1	1	2
dijeli r_2 sa x^2 i podesi u_1				
$x^4 + x^2 + 1$	$x^5 + x^2 + x + 1$	x^2	1	4
postavi $r_2 = r_2 + r_1$ i $u_2 = u_2 + u_1$				
$x^4 + x^2 + 1$	$x^5 + x^4 + x$	x^2	$x^2 + 1$	4
dijeli r_2 sa x^1 i podesi u_1				
$x^4 + x^2 + 1$	$x^4 + x^3 + 1$	x^3	$x^2 + 1$	5
postavi $r_1 = r_1 + r_2$ i $u_1 = u_1 + u_2$				
$x^3 + x^2$	$x^4 + x^3 + 1$	$x^3 + x^2 + 1$	$x^2 + 1$	5
dijeli r_1 sa x^2 i podesi u_2				
$x + 1$	$x^4 + x^3 + 1$	$x^3 + x^2 + 1$	$x^4 + x^2$	7
postavi $r_2 = r_2 + r_1$ i $u_2 = u_2 + u_1$				
$x + 1$	$x^4 + x^3 + x$	$x^3 + x^2 + 1$	$x^4 + x^3 + 1$	7
dijeli r_2 sa x^1 i podesi u_1				
$x + 1$	$x^3 + x^2 + 1$	$x^4 + x^3 + x$	$x^4 + x^3 + 1$	8
postavi $r_2 = r_2 + r_1$ i $u_2 = u_2 + u_1$				
$x + 1$	$x^3 + x^2 + x$	$x^4 + x^3 + x$	$x + 1$	8
dijeli r_2 sa x^1 i podesi u_1				
$x + 1$	$x^2 + x + 1$	$x^5 + x^4 + x^2$	$x + 1$	9
postavi $r_2 = r_2 + r_1$ i $u_2 = u_2 + u_1$				
$x + 1$	x^2	$x^5 + x^4 + x^2$	$x^5 + x^4 + x^2 + x + 1$	9
dijeli r_2 sa x^2 i podesi u_1				
$x + 1$	1	$x^7 + x^6 + x^4$	$x^5 + x^4 + x^2 + x + 1$	11

Petlja se prekida zbog $r_2 = 1$. *U tom trenutku* $k = 11$ *i* $u_2 = x^5 + x^4 + x^2 + x + 1$. *Dakle, izračunavamo* $x^{-11}\left(x^5 + x^4 + x^2 + x + 1\right)$ *modulo* f *za* $f(x) = x^7 + x^3 + 1$.

l	h	$u + hf$	$(u + hf)/x^l = u$
			$x^5 + x^4 + x^2 + x + 1$
3	$x^2 + x + 1$	$x^9 + x^8 + x^7 + x^3$	$x^6 + x^5 + x^4 + 1$
3	1	$x^7 + x^6 + x^5 + x^4 + x^3$	$x^4 + x^3 + x^2 + x + 1$
2	$x + 1$	$x^8 + x^7 + x^2$	$x^6 + x^5 + 1$
3	1	$x^7 + x^6 + x^5 + x^3$	$x^4 + x^3 + x^2 + 1$

Bibliografija

[1] A. Das, *Computational Number Theory*, CRC Press, 2013.

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

[3] Y. Kawahara, K. Aoki i T. Takagi, *Faster Implementation of η_T Pairing over GF* (3^m) *Using Minimum Number of Logical Instructions for GF(3)-Addition*, Pairing-Based Cryptography – Pairing 2008, Springer Berlin Heidelberg, 2008, str. 282–296.

[4] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, 1994.

[5] R. Lidl i H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 1986.

[6] B. Širola, *Algebarske strukture*, `https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf`, posjećena 05.09.2022.

Sažetak

U ovom radu smo obradili pitanja reprezentacije elemenata u konačnim poljima te efiksne implementacije operacija na konačnim poljima. Na početku smo se prisjetili osnovnih algebarskih struktura - grupa, prstena i polja. Uveli smo pojam konačnog, prostog i proširenog polja. Konačna polja smo reprezentirali ireducibilnim polinomima. Pokazali smo kako u programskom paketu PARI/GP odraditi aritmetičke operacije na polinomima iz $\mathbb{F}_2[x]$. Objasnili smo kako odabrati definirajući polinom nekog proširenog polja $\mathbb{F}_{p^n}$. Pokazali smo kako implementirati zbrajanje, oduzimanje i množenje u proširenim poljima karakteristike 2 i 3. Za algoritam množenja smo pojasnili ubrzanje algoritma u vidu češalj metoda. Dali smo algoritam za modularnu redukciju. Dali smo algoritme za računanje inverza - Euklidov i binarni te ubrzanje binarnog.

Summary

In this paper, we dealt with the issues of representation of elements in finite fields and efficient implementation of operations on finite fields. At the beginning, we remind ourselves of the basic algebraic structures - groups, rings and fields. We have introduced the concept of finite, prime and extended field. We represented the finite fields with irreducible polynomials. We have shown how to perform arithmetic operations on polynomials from $\mathbb{F}_2[x]$ in the program package PARI/GP. We explained how to choose defining polynomial of some extended field $\mathbb{F}_{p^n}$. We have shown how to implement addition, subtraction and multiplication in the extended fields of characteristics 2 and 3. For the multiplication algorithm, we have clarified the acceleration of the algorithm in the form of comb methods. We have provided an algorithm for modular reduction. We have provided algorithms for calculating the inverse - Euclidean and binary and acceleration of the binary.

Životopis

Rođen sam 18. siječnja 1995. godine u Požegi. Nakon osnovne škole, koju sam pohađao u Velikoj, 2009. godine upisao sam Prirodoslovno-matematičku gimnaziju u Požegi. Zbog sudjelovanja na Državnom natjecanju iz matematike 2012. godine stječem izravan upis na preddiplomski sveučilišni studij Matematike na PMF-u na kojem 2013. godine započinjem studiranje. Nakon stjecanja diplome sveučilišnog prvostupnika upisao sam diplomski sveučilišni studij Matematike, smjer Računarstvo i matematika. Od 2021. godine radim u Ericsson Nikola Tesla na mjestu 5G software developera.