Uvod u računarstvo
5. predavanje

Saša Singer

singer@math.hr

web.math.hr/~singer

PMF – Matematički odjel, Zagreb

Sadržaj predavanja

Prvi dio je ponavljanje zadnjeg dijela prošlog predavanja.

- Cijeli brojevi — prikaz i aritmetika:
  - prikaz brojeva bez predznaka,
  - modularna aritmetika cijelih brojeva,
  - prsten ostataka modulo 2^n,
  - dijeljenje s ostatkom — Euklidov teorem,
  - prikaz brojeva bez predznaka — sustav ostataka,
  - prikaz brojeva s predznakom — sustav ostataka,
  - prikaz negativnih brojeva — komplementiraj i dodaj 1,
  - tipične pogreške u korištenju cijelih brojeva.

Sadržaj predavanja (nastavak)

- Prikaz realnih brojeva — “floating–point” standard:
  - osnovni oblik “floating–point” prikaza — mantisa i eksponent,
  - greške zaokruživanja u prikazu,
  - pojam “jedinične greške zaokruživanja”,
  - IEEE standard — tipovi: single, double, extended.

Prikaz cijelih brojeva u računalu

Sadržaj predavanja

Prvi dio je ponavljanje zadnjeg dijela prošlog predavanja.

- Cijeli brojevi — prikaz i aritmetika:
  - prikaz brojeva bez predznaka,
  - modularna aritmetika cijelih brojeva,
  - prsten ostataka modulo 2^n,
  - dijeljenje s ostatkom — Euklidov teorem,
  - prikaz brojeva bez predznaka — sustav ostataka,
  - prikaz brojeva s predznakom — sustav ostataka,
  - prikaz negativnih brojeva — komplementiraj i dodaj 1,
  - tipične pogreške u korištenju cijelih brojeva.

Prikaz cijelih brojeva bez predznaka

Ponavljanje. Ako imamo n bitova za prikaz brojeva, onda je skup svih prikazivih cijelih brojeva bez predznaka jednak

$$\{\, 0,\ 1,\ 2,\ \ldots\ ,\ 2^n - 2,\ 2^n - 1 \,\}$$

i ima 2^n elemenata. Prikaz (prikazivog) broja B je

$$\mathrm{bit}_i = b_i, \quad \text{za} \quad i = 0, \ldots , n-1,$$

gdje je

$$B = b_{n-1} \cdot 2^{n-1} + \cdots + b_1 \cdot 2 + b_0, \quad b_i \in \{0, 1\},$$

tzv. "prošireni" zapis tog broja B u bazi 2, s točno n binarnih znamenki, s tim da vodeće znamenke smiju biti jednake 0.

Aritmetika cijelih brojeva bez predznaka

Aritmetika cijelih brojeva bez predznaka s n bitova za prikaz brojeva je aritmetika ostataka modulo 2^n.

To znači da aritmetičke operacije $+$, $-$ i $\cdot$ na skupu cijelih brojeva bez predznaka daju rezultat koji je

- jednak ostatku rezultata pripadne cjelobrojne operacije (u skupu $\mathbb{Z}$) pri dijeljenju s 2^n.

Drugim riječima, za prikazive operande A i B vrijedi

$$\text{rezultat } (A \text{ op } B) := (A \text{ op } B) \bmod 2^n,$$

gdje je op zbrajanje, oduzimanje ili množenje.

Aritmetika cijelih brojeva bez predznaka

Dakle, rezultat operacije ne mora biti isti kao da smo na "modelnom" skupu $\mathbb{N}_0$ ili $\mathbb{Z}$.

Primjer. Kad najvećem prikazivom broju $2^n - 1$ dodamo 1, rezultat je nula, jer je

$$(2^n - 1) + 1 = ((2^n - 1) + 1) \bmod 2^n = 2^n \bmod 2^n = 0.$$

Analogno, $2 \cdot 2^{n-1} = 0$, ali tek uz uvjet $n > 1$ (inače broj 2 nije prikaziv).

Matematički cilj ovakve definicije aritmetike:

- dobiti "dobru" algebarsku strukturu na cijelim brojevima bez predznaka.

Isto vrijedi i za cijele brojeve s predznakom.

Aritmetika cijelih brojeva bez predznaka

Za početak, uočite:

- rezultat ovako definiranih operacija je uvijek prikaziv,

što znači da je skup svih prikazivih cijelih brojeva bez predznaka zatvoren obzirom na ove operacije.

Iako cijeli brojevi bez predznaka modeliraju skup $\mathbb{N}_0$, taj skup ima "preslabu" strukturu (nema oduzimanja), pa se struktura modelira prema skupu $\mathbb{Z}$ (prsten s jedinicom).

- U pozadini ove realizacije aritmetike je klasična algebarska struktura prstena ostataka modulo 2^n.

Tu strukturu je korisno detaljnije opisati, jer bitno olakšava razumijevanje cjelobrojne aritmetike (i one s predznakom).

Prsten ostataka modulo 2^n

Naime, skup svih prikazivih cijelih brojeva bez predznaka

$$\mathbb{Z}_{2^n} = \{\, 0,\ 1,\ 2,\ \ldots\ ,\ 2^n - 2,\ 2^n - 1 \,\}$$

je ujedno i standardni sustav ostataka koji dobivamo pri cjelobrojnom dijeljenju s 2^n. Zato se i označava sa $\mathbb{Z}_{2^n}$.

Ako na njemu definiramo binarne operacije zbrajanja $\oplus$ i množenja $\odot$ preko ostataka cjelobrojnih operacija $+$ i $\cdot$,

$$A \oplus B := (A + B) \bmod 2^n,$$

$$A \odot B := (A \cdot B) \bmod 2^n,$$

onda $(\mathbb{Z}_{2^n}, \oplus, \odot)$ ima algebarsku strukturu prstena s 1.

U algebri se operacije $\oplus$ i $\odot$ obično označavaju s $\oplus_{2^n}$ i $\odot_{2^n}$.

Prsten ostataka modulo 2^n (nastavak)

Što znači da je $(\mathbb{Z}_{2^n}, \oplus, \odot)$ prsten s jedinicom? Vrijedi:

- $(\mathbb{Z}_{2^n}, \oplus)$ je komutativna grupa (obzirom na zbrajanje),
- $(\mathbb{Z}_{2^n}, \odot)$ je polugrupa (obzirom na množenje), čak i monoid, jer ima jedinicu $1 \in \mathbb{Z}_{2^n}$,
- operacije $\oplus$ i $\odot$ vezane su zakonom distributivnosti, tj.

$$A \odot (B \oplus C) = A \odot B \oplus A \odot C,$$
$$(A \oplus B) \odot C = A \odot C \oplus B \odot C,$$

  za svaki izbor A, B, $C \in \mathbb{Z}_{2^n}$.

Dodatno, $(\mathbb{Z}_{2^n}, \oplus, \odot)$ je i komutativni prsten s jedinicom, ali nije polje (za $n > 1$), jer ima djelitelja nule $(2 \cdot 2^{n-1} = 0)$.

Prsten ostataka modulo 2^n (nastavak)

Neka je "$-A$" jedinstveni suprotni element elementa A obzirom na zbrajanje. Očito je "-0" $= 0$, a za $A \neq 0$ vrijedi "$-A$" $= 2^n - A$, jer je

$$A \oplus \text{“}-A\text{”} = (A + (2^n - A)) \bmod 2^n = 0.$$

Na kraju, oduzimanje $\ominus$ definiramo kao zbrajanje sa suprotnim elementom

$$A \ominus B := A + \text{“}-B\text{”}.$$

I tako smo dobili tri osnovne aritmetičke operacije na $\mathbb{Z}_{2^n}$, koje se upravo na taj način realiziraju u računalu za cijele brojeve bez predznaka. U programskim jezicima se ove tri operacije pišu znakovima $+$, $-$ i $*$ (za $\cdot$, odnosno $\odot$).

Dijeljenje cijelih brojeva

A što je s dijeljenjem? To dosad nismo ni spomenuli!

S razlogom! "Obično" dijeljenje ima smisla tek u strukturi polja, poput racionalnih brojeva $\mathbb{Q}$ ili realnih brojeva $\mathbb{R}$.

Znamo da $\mathbb{N}_0$ i $\mathbb{Z}$ nisu polja. Isto vrijedi i za $\mathbb{Z}_{2^n}$, čim je $n > 1$, a slučaj $n = 1$ je potpuno neinteresantan za praksu, barem što se tiče aritmetike cijelih brojeva (iako je vrlo bitan za logičku algebru).

Što sad?

Zamjena za "obično" dijeljenje u cijelim brojevima je tzv. dijeljenje s ostatkom. Podloga za to je poznati Euklidov teorem o dijeljenju s ostatkom u skupu $\mathbb{Z}$.

Dijeljenje cijelih brojeva — Euklidov teorem

Euklidov teorem. Za svaki cijeli broj $a \in \mathbb{Z}$ i svaki prirodni broj $b \in \mathbb{N}$, postoje jedinstveni brojevi q, $r \in \mathbb{Z}$, takvi da je

$$a = q \cdot b + r \quad \text{i} \quad 0 \leq r < b.$$

Broj q je cjelobrojni kvocijent, a r ostatak pri dijeljenju a s b.

Ograničenje $0 \leq r < b$ znači da za ostatak r vrijedi

$$r \in \mathbb{Z}_b := \{\, 0,\ 1,\ 2,\ \ldots\ ,\ b - 1 \,\},$$

pa skup $\mathbb{Z}_b$ zovemo standardni sustav ostataka modulo b.

Zvuči poznato: ako uzmemo divizor $b = 2^n$, dobivamo skup svih prikazivih cijelih brojeva bez predznaka u računalu.

Dijeljenje cijelih brojeva — dvije operacije

Uočite da Euklidov teorem, odnosno, cjelobrojno dijeljenje s ostatkom daje dva rezultata:

- cjelobrojni kvocijent i ostatak.

Zgodno je odmah uvesti i oznake za obje ove operacije.

Nažalost, nema standardne matematičke oznake za cjelobrojni kvocijent. Oznaka / standardno se koristi za operaciju "običnog" dijeljenja u poljima, ili se pišu razlomci. Kad napišem

$$a/b \qquad \text{ili} \qquad \frac{a}{b}$$

to odmah asocira na obično dijeljenje (što nije zgodno).

Oznake za cjelobrojni kvocijent i ostatak

S druge strane, u nekim programskim jezicima (C, Fortran) oznaka / se koristi i za cjelobrojno dijeljenje, ali to vrijedi

- ako i samo ako su oba operanda cijeli brojevi.

Usput, isti princip da tip rezultata ovisi o tipu oba operanda (tzv. "operator overloading") vrijedi i za tri ranije operacije s oznakama $+$, $-$, $*$.

Da izbjegnemo mogućnost bilo kakve zabune,

- za cjelobrojni kvocijent koristimo oznaku div, po ugledu na Pascal (oznaka / u C-u),
- a za ostatak postoji standardna oznaka mod, koju smo već koristili (oznaka % u C-u).

Definicija operacija za cjelobrojno dijeljenje

Precizna definicija ovih operacija izlazi direktno iz Euklidovog teorema.

Definicija. Neka su $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ bilo koji brojevi, i neka su $q \in \mathbb{Z}$ (cjelobrojni kvocijent) i $r \in \mathbb{Z}_b$ (ostatak) jedinstveni brojevi za koje vrijedi

$$a = q \cdot b + r.$$

Operacije div i mod definiramo relacijama

$$a \operatorname{div} b := q \in \mathbb{Z}, \qquad a \operatorname{mod} b := r \in \mathbb{Z}_b.$$

Ova definicija operacije mod točno odgovara onom što smo ranije koristili.

Dijeljenje cijelih brojeva — mala digresija

Za početak, uočite da su obje operacije definirane na skupu $\mathbb{Z} \times \mathbb{N}$, a kodomene su različite.

Možda nekog zanima što se zbiva na skupu $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$,

- kad cjelobrojno dijelimo dva cijela broja (što, naravno, ima smisla).

O tome malo kasnije, kod cijelih brojeva s predznakom. Odmah jedno upozorenje:

- stvar radi očekivano (prema Euklidovom teoremu) samo na skupu $\mathbb{N}_0 \times \mathbb{N}$.

Trenutno nam upravo taj skup i treba, da dobijemo cjelobrojno dijeljenje za cijele brojeve bez predznaka (koji modeliraju $\mathbb{N}_0$).

Veza cjelobrojnog i običnog dijeljenja

Zahtjev da je $0 \leq r < b$, tj. da ostatak r pripada skupu $\mathbb{Z}_b$, daje jednostavnu vezu cjelobrojnog i običnog dijeljenja (onog u racionalnim brojevima).

Lako se vidi da vrijedi

$$a \operatorname{div} b = q = \left\lfloor \frac{a}{b} \right\rfloor .$$

Dakle, cjelobrojni kvocijent je "najveće cijelo" od običnog (racionalnog) kvocijenta.

Ova veza je specifična za izbor $r \in \mathbb{Z}_b$ i ne vrijedi za drugačije sustave ostataka (a takve sustave možemo izabrati, kao što ćemo vidjeti).

Prsten ostataka modulo b

Za bilo koji fiksni divizor $b \geq 2$, na standardnom sustavu ostataka modulo b, tj. skupu

$$\mathbb{Z}_b = \{\, 0,\ 1,\ 2,\ \ldots\ ,\ b-1 \,\}$$

možemo definirati binarne operacije zbrajanja $\oplus_b$ i množenja $\odot_b$ preko ostataka cjelobrojnih operacija $+$ i $\cdot$,

$$A \oplus_b B := (A + B) \bmod b,$$

$$A \odot_b B := (A \cdot B) \bmod b.$$

Lako se dokazuje da $(\mathbb{Z}_b, \oplus_b, \odot_b)$ ima algebarsku strukturu komutativnog prstena s jedinicom (kao i ranije za $b = 2^n$).

Ta struktura je polje ako i samo ako je b prost broj.

Dijeljenje cijelih brojeva bez predznaka

Sve što smo dosad rekli o cjelobrojnom dijeljenju s ostatkom (zasad) vrijedi

- samo za cijele brojeve, ili, preciznije, na $\mathbb{Z} \times \mathbb{N}$.

Taj skup je "domena" za Euklidov teorem. Stoga su operacije div i mod definirane baš na toj domeni.

A što je s cjelobrojnim dijeljenjem s ostatkom u računalu, tj. na skupu $\mathbb{Z}_{2^n}$ prikazivih cijelih brojeva bez predznaka?

Odgovor: Potpuno isto kao da smo u cijelim brojevim.

Drugim riječima, dijeljenje s ostatkom cijelih brojeva bez predznaka je naprosto

- restrikcija "cjelobrojnih" operacija div i mod.

Dijeljenje cijelih brojeva bez predznaka

Zašto? Uzmimo bilo koji fiksni divizor $b \geq 2$.

Neka su $A \in \mathbb{Z}_b$ i $B \in \mathbb{Z}_b$, $B > 0$, bilo koji brojevi iz $\mathbb{Z}_b$ koje "smijemo dijeliti". Podijelimo ih cjelobrojno, i pokažimo da su kvocijent $Q := A \operatorname{div} B$ i ostatak $R := A \bmod B$ opet u skupu $\mathbb{Z}_b$.

Znamo da općenito vrijedi $Q \in \mathbb{Z}$, $R \in \mathbb{Z}_B$ (tj. $0 \leq R < B$) i

$$A = Q \cdot B + R.$$

Zbog $0 \leq A, B < b$, odmah vidimo da je

$$0 \leq Q < b \quad \text{i} \quad 0 \leq R < B < b,$$

što dokazuje $Q,\ R \in \mathbb{Z}_b$.

Dijeljenje cijelih brojeva bez predznaka

Naravno, cijela stvar vrijedi i za $b = 2^n$.

Zbog toga, dijeljenje s ostatkom u skupu $\mathbb{Z}_{2^n}$ prikazivih cijelih brojeva bez predznaka u računalu

- daje potpuno iste rezultate kao da dijelimo u $\mathbb{Z}$ (ili $\mathbb{N}_0$).

Dakle, nema ostataka modulo 2^n i "čarolija" s prikazivošću rezultata.

Operacije div i mod su jedine aritmetičke operacije koje na prikazivim cijelim brojevima bez predznaka $\mathbb{Z}_{2^n}$ daju iste rezultate kao i na skupu $\mathbb{N}_0$ kojeg modeliramo.

Ponovimo još jednom da ostale tri operacije $+$, $-$ i $\cdot$

- daju cjelobrojni rezultat modulo 2^n.

Euklidov teorem u prstenu ostataka modulo b

Uočite da za operacije div i mod na skupu $\mathbb{Z}_b$ koristimo Euklidov teorem za cijele brojeve, tj. na domeni $\mathbb{Z} \times \mathbb{N}$.

Pitanje: Kad znamo da je $(\mathbb{Z}_b, \oplus_b, \odot_b)$ prsten, kao i $(\mathbb{Z}, +, \cdot)$, zašto ne uzmemo "prirodniju" domenu $\mathbb{Z}_b \times (\mathbb{Z}_b \setminus \{0\})$?

Odgovor: Na toj domeni, s pripadnim modularnim operacijama $\oplus_b$ i $\odot_b$, također, vrijedi Euklidov teorem, ali nema jedinstvenosti rezultata.

Euklidov teorem u prstenu $(\mathbb{Z}_b, \oplus_b, \odot_b)$. Za svaka dva broja $A, B \in \mathbb{Z}_b$, $B > 0$, postoje brojevi $Q, R \in \mathbb{Z}_b$, takvi da je

$$A = Q \odot_b B \oplus_b R \quad \text{i} \quad 0 \leq R < B,$$

ali ti brojevi ne moraju biti jedinstveni.

Euklidov teorem u prstenu ostataka modulo b

Primjer. Uzmimo $b = 2^3 = 8$, tj. prsten $(\mathbb{Z}_8, \oplus_8, \odot_8)$, i brojeve $A = 5$, $B = 4$. Onda je (kao u cijelim brojevima)

$$5 = 1 \cdot 4 + 1,$$

tj. $5 \operatorname{div} 4 = 1$, $5 \bmod 4 = 1$. Ali, zbog $2 \odot_8 4 = 0 \bmod 8$, vrijedi i

$$5 = 3 \odot_8 4 \oplus_8 1 = 13 \bmod 8,$$

$$5 = 5 \odot_8 4 \oplus_8 1 = 21 \bmod 8,$$

$$5 = 7 \odot_8 4 \oplus_8 1 = 29 \bmod 8.$$

Dakle, “modularni” kvocijenti su 1, 3, 5 i 7, a najmanji je pravi.

Cijeli brojevi bez predznaka — sažetak

Ako imamo n bitova za prikaz brojeva, onda je skup svih prikazivih cijelih brojeva bez predznaka jednak

$$\mathbb{Z}_{2^n} = \{\, 0,\ 1,\ 2,\ \ldots\ ,\ 2^n - 2,\ 2^n - 1\,\}.$$

Prikaz broja $B \in \mathbb{Z}_{2^n}$ dobiva se iz "proširenog" zapisa tog broja u bazi 2, s točno n binarnih znamenki.

Aritmetika cijelih brojeva bez predznaka je modularna aritmetika u prstenu $(\mathbb{Z}_{2^n}, \oplus_{2^n}, \odot_{2^n})$:

- operacije $+$, $-$ i $\cdot$ daju cjelobrojni rezultat modulo 2^n,
- operacije cjelobrojnog dijeljenja s ostatkom div i mod daju iste rezultate kao da dijelimo u $\mathbb{Z}$ (ili $\mathbb{N}_0$).

Cijeli brojevi u C-u — sažetak

U programskom jeziku C:

- cijelim brojevima bez predznaka odgovara tip koji se zove `unsigned int`,
- cijelim brojevima s predznakom odgovara tip koji se zove `int`.

Ovi tipovi postoje u nekoliko raznih veličina

- standardna, `short`, `long`, a katkad i druge.

Razlike su u broju bitova n predviđenih za prikaz.

- Zapis konstanti (vrijednost, navođenje tipa).
- Zapis operacija $+$, $-$ i $\cdot$ znakovima $+$, $-$ i $*$.
- Zapis operacija div i mod znakovima $/$ i $\%$

Cijeli brojevi bez predznaka u C-u — primjer 1

```
#include <stdio.h>

int main(void) {
    unsigned short i=65535;  /* int ne pisem */

    printf("%d\n", i/10);  /* 6553 */

    i=i+3;
    printf("%d\n", i);     /* 2, a ne 65538 */

    return 0;
}
```

`USHRT_MAX = 65535` u zaglavlju `limits.h`

Cijeli brojevi bez predznaka u C-u — primjer 2

```
#include <stdio.h>

int main(void) {
    unsigned short i=2, j=4;

    i=i-j;
    printf("%d\n", i);  /* 65534, a ne -2 */

    return 0;
}
```

Cijeli brojevi u C-u — sažetak

Primjer C programa za prikaz brojeva i čitanje brojeva.

Kod čitanja, pretvorba iz niza znakova (dekadske znamenke u dekadskom zapisu) u binarni zapis ide onim aritmetičkim pravilima koja odgovaraju TIPU broja ("Hornerov" algoritam).

Cijeli brojevi s predznakom

Cijeli brojevi s predznakom modeliraju skup $\mathbb{Z}$ cijelih brojeva.

Ako imamo n bitova na raspolaganju za prikaz, onda skup prikazivih brojeva ima 2^n elemenata.

Među prikazivim brojevima moraju biti i (neki) negativni brojevi. Zgodno bi bilo da ih je podjednako mnogo kao i pozitivnih (odnosno, nenegativnih) brojeva.

Standardni dogovor: u računalu se prikazuje

- najveći mogući podskup uzastopnih brojeva iz $\mathbb{Z}$ koji je "skoro" simetričan oko 0.

"Prava" simetrija bi dala neparan broj prikazivih brojeva.

Cijeli brojevi s predznakom (nastavak)

To osigurava da negativnih brojeva ima podjednako mnogo kao i nenegativnih.

Ako želimo da polovina tih brojeva bude negativna, onda njih mora biti točno 2^{n-1}. Nenegativnih brojeva je, naravno, isto toliko.

To znači da je skup svih prikazivih cijelih brojeva s predznakom jednak

$$\mathbb{Z}_{2^n}^{-} = \{ -2^{n-1}, \ -2^{n-1}+1, \ \ldots\ , -1, \\ 0, \ 1, \ \ldots\ , \ 2^{n-1}-2, \ 2^{n-1}-1 \}.$$

Brojeve izvan tog skupa ne možemo prikazati sa samo n bitova.

Cijeli brojevi s predznakom (nastavak)

Najmanji i najveći prikazivi cijeli broj s predznakom su, redom

$$-2^{n-1}, \quad 2^{n-1} - 1.$$

Tipične vrijednosti za ta dva "granična" broja su:

n	-2^{n-1}	$2^{n-1} - 1$
8	-128	127
16	$-32\,768$	32 767
32	$-2\,147\,483\,648$	2 147 483 647

Uočite da raspon prikazivih cijelih brojeva s predznakom nije jako velik, čak i za $n = 32$ (standard). Oprez!

Zato se danas sve više koristi $n = 64$ (želja za $n = 128$).

Cijeli brojevi s predznakom (nastavak)

Kako stvarno izgleda prikaz brojeva u tih n bitova?

Prikaz pojedinih (prikazivih) brojeva potpuno je određen s dva zahtjeva:

- nenegativni brojevi imaju isti prikaz kao u cijelim brojevima bez predznaka (dovoljno je to tražiti samo za jedan broj, na primjer, nulu),
- aritmetika za te prikaze mora (kao i ranije, za brojeve bez predznaka) dati “dobru” algebarsku strukturu na cijelim brojevima s predznakom.

Prvi zahtjev je dosta jasan, ali što znači drugi?

Cijeli brojevi s predznakom (nastavak)

Kod brojeva bez predznaka, prikaz binarnim znamenkama je očito odgovarao aritmetici — recimo, ovako:

- kad prikazu broja B (kao nizu bitova u bazi 2) dodamo 1, dobijemo točno prikaz broja $B + 1$.

(Hm, nismo baš puno razmišljali o tome).

Modularna aritmetika modulo 2^n dodatno još "zatvara krug" na n bitova, tj. daje zatvorenost operacija, a onda i dobru strukturu prstena s jedinicom na $\mathbb{Z}_{2^n} = \{\, 0,\ 1,\ \ldots\ ,\ 2^n - 1 \,\}$.

Zato gore, umjesto običnog cjelobrojnog $+$, koristimo $\oplus_{2^n}$.

Potpuno isto mora vrijediti i za prikaze cijelih brojeva s predznakom — inače nemamo jednostavnu realizaciju aritmetike i dobru strukturu.

Cijeli brojevi s predznakom (nastavak)

Dakle, aritmetika za cijele brojeve s predznakom mora i dalje biti ista, tj.

- modularna aritmetika modulo 2^n,

samo je interpretacija sustava ostataka drugačija.

Skup svih prikazivih cijelih brojeva s predznakom

$$\mathbb{Z}_{2^n}^{-} = \{ -2^{n-1}, \ldots, -1, 0, 1, \ldots, 2^{n-1} - 1 \}$$

je, također, potpuni sustav ostataka modulo 2^n.

Na tom skupu opet možemo definirati operacije zbrajanja i množenja (bez posebnih oznaka) preko odgovarajućih ostataka cjelobrojnih operacija $+$ i $\cdot$. Kao i prije, dobivamo strukturu prstena s jedinicom.

Cijeli brojevi s predznakom (nastavak)

A sad je lako dobiti prikaz svih negativnih brojeva.

Usporedimo skupove prikazivih brojeva bez predznaka i s predznakom, tj. pripadne sustave ostataka modulo 2^n),

$$\mathbb{Z}_{2^n} = \{\, 0,\ 1,\ \ldots\ ,\ 2^n - 1 \,\},$$
$$\mathbb{Z}_{2^n}^{-} = \{\, -2^{n-1},\ \ldots\ , -1,\ 0,\ 1,\ \ldots\ ,\ 2^{n-1} - 1 \,\}.$$

- Prvo "poklopimo" zajednički dio nenegativnih brojeva $0, \ldots, 2^{n-1} - 1$. Njihovi prikazi su isti!
  - Uočite da svi oni imaju vodeći bit jednak 0.
- Zatim "zatvaramo krug" dodavanjem jedan po jedan modulo 2^n i "sparujemo" odgovarajuće brojeve.

Cijeli brojevi s predznakom (nastavak)

Prvi "dodaj jedan" modulo 2^n daje

$$((2^{n-1}-1)+1) \bmod 2^n = 2^{n-1} \bmod 2^n = \begin{cases} 2^{n-1} \in \mathbb{Z}_{2^n}, \\ -2^{n-1} \in \mathbb{Z}_{2^n}^-, \end{cases}$$

tj. zatvara krug u $\mathbb{Z}_{2^n}^-$, pa "sparujemo"

$$-2^{n-1} \in \mathbb{Z}_{2^n}^- \quad \leftrightarrow \quad 2^{n-1} \in \mathbb{Z}_{2^n}.$$

A dalje sve ide redom. Kad to ponovimo k puta, tj. dodamo k modulo 2^n, izlazi:

$$-2^{n-1}+(k-1) \in \mathbb{Z}_{2^n}^- \quad \leftrightarrow \quad (2^{n-1}-1)+k \in \mathbb{Z}_{2^n},$$

za $k = 1, \ldots, 2^{n-1}$.

Cijeli brojevi s predznakom (nastavak)

Kad ovu relaciju malo preuredimo, supstitucijom za negativne brojeve $-B = -2^{n-1} + (k-1)$, dobivamo

$$-B \in \mathbb{Z}_{2^n}^- \quad \leftrightarrow \quad 2^n - B \in \mathbb{Z}_{2^n},$$

i to vrijedi za $B = 1, \ldots, 2^{n-1}$.

Dakle, spareni brojevi se razlikuju za točno 2^n.

To je jasno, jer moraju imati isti “pravi” ostatak modulo 2^n.

Zaključak: za $B = 1, \ldots, 2^{n-1}$,

- prikaz negativnog broja $-B$ (s predznakom)
- jednak je prikazu broja $2^n - B$ (bez predznaka).

Cijeli brojevi s predznakom (nastavak)

Primjer. Prikaz broja -2^{n-1} dobivamo tako da uzmemo $B = 2^{n-1}$ (koji sam nije prikaziv s predznakom) i pogledamo prikaz broja $2^n - B$ bez predznaka:

$$-2^{n-1} \quad \leftrightarrow \quad 2^n - 2^{n-1} = 2^{n-1} = [\,1\ 0\ 0\ \ldots\ 0\ 0\,].$$

Ovdje koristimo skraćenu oznaku

$$[\,\mathrm{bit}_{n-1}\ \mathrm{bit}_{n-2}\ \mathrm{bit}_{n-3}\ \ldots\ \mathrm{bit}_1\ \mathrm{bit}_0\,]$$

za zapis vrijednosti svih n bitova u prikazu broja.

Primjer. Broj -1 ima prikaz $(B = 1)$

$$-1 \quad \leftrightarrow \quad 2^n - 1 = [\,1\ 1\ 1\ \ldots\ 1\ 1\,].$$

Cijeli brojevi s predznakom (nastavak)

Primjer. Kad najvećem prikazivom broju (s predznakom) $2^{n-1} - 1$ dodamo 1, rezultat je najmanji prikazivi broj (s predznakom), jer je

$$\begin{aligned}(2^{n-1} - 1) + 1 &= ((2^{n-1} - 1) + 1) \bmod 2^n \\ &= 2^{n-1} \bmod 2^n = -2^{n-1} \in \mathbb{Z}^-_{2^n}.\end{aligned}$$

Naravno, isti rezultat izlazi i običnim binarnim "zbrajanjem prikaza"

$$[0\ 1\ 1\ \ldots\ 1\ 1] + [0\ 0\ 0\ \ldots\ 0\ 1] = [1\ 0\ 0\ \ldots\ 0\ 0].$$

Uočite da nema prijenosa.

Cijeli brojevi s predznakom (nastavak)

Primjer. Analogno, zbrajanju $(-1) + 1 = 0$ odgovara binarno "zbrajanje prikaza"

$$[1\ 1\ 1\ \ldots\ 1\ 1] + [0\ 0\ 0\ \ldots\ 0\ 1] = 1\ [0\ 0\ 0\ \ldots\ 0\ 0].$$

Ovdje imamo prijenos, ali se on "modularno" ignorira.

Cijeli brojevi s predznakom (nastavak)

Dakle, prikaz negativnih brojeva je posljedica one iste modularne aritmetike koja vrijedi i za cijele brojeve bez predznaka.

Tehnički gledano, tri osnovne operacije $+$, $-$ i $\cdot$ na cijelim brojevima u računalu se izvršavaju

- potpuno jednako (istim "elektroničkim krugovima") za cijele brojeve s predznakom i bez njega,

Važni su samo bitovi u prikazu, a ne i njihova interpretacija!

Za cjelobrojno dijeljenje to ne vrijedi (v. malo kasnije).

Vodeći bit — predznak

U prikazu cijelih brojeva s predznakom

- svi nenegativni brojevi imaju vodeći bit jednak 0, a
- svi negativni brojevi imaju vodeći bit jednak 1.

Zato se vodeći bit obično zove i bit predznaka (engl. sign).

Taj naziv, nažalost, može zavesti na pogrešnu ideju o prikazu. Prikaz cijelih brojeva s predznakom se ne dobiva kao:

- bit predznaka i prikaz apsolutne vrijednosti broja (bez predznaka, s bitom manje).

Za razliku od ovog, kod "realnih" brojeva to vrijedi, što samo povećava mogućnost zabune.

Veza broja i prikaza s predznakom

Zasad znamo da za prikaz cijelih brojeva s predznakom vrijedi:

- nenegativni brojevi $B = 0, \ldots, 2^{n-1} - 1$ imaju isti prikaz kao i bez predznaka,
- negativni brojevi $B = -1, \ldots, -2^{n-1}$ imaju isti prikaz kao i brojevi $2^n + B$ bez predznaka.

Tj., imamo dva različita slučaja, ovisno o "predznaku" broja.

Da bismo dobili vezu između n bitova u prikazu broja B s predznakom i samog broja, postupamo na sljedeći način.

Broju $B \in \mathbb{Z}_{2^n}^-$ pridružimo broj $B' \in \mathbb{Z}_{2^n}$, tako da B s predznakom ima isti prikaz na n bitova kao i broj B' bez predznaka. Taj broj B' označavamo s $\text{prikaz}(B)$.

Veza broja i prikaza s predznakom (nastavak)

Već znamo da je

$$\mathrm{prikaz}(B) = \begin{cases} B, & \text{za} \quad B = 0, \ldots, 2^{n-1} - 1, \\ 2^n + B, & \text{za} \quad B = -1, \ldots, -2^{n-1}. \end{cases}$$

Nama treba "obratna" veza:

$$B = \begin{cases} \mathrm{prikaz}(B), & \text{za} \quad \mathrm{prikaz}(B) = 0, \ldots, 2^{n-1} - 1, \\ \mathrm{prikaz}(B) - 2^n, & \text{za} \quad \mathrm{prikaz}(B) = 2^{n-1}, \ldots, 2^n - 1, \end{cases}$$

jer $\mathrm{prikaz}(B)$ ima jednostavnu vezu sa svojim bitovima.

A onda je lako.

Veza broja i prikaza s predznakom (nastavak)

Neka je

$$[\,\mathrm{bit}_{n-1}\ \mathrm{bit}_{n-2}\ \ldots\ \mathrm{bit}_1\ \mathrm{bit}_0\,]$$

zapis prikazivog cijelog broja $B \in \mathbb{Z}_{2^n}^-$ s predznakom, gdje su $\mathrm{bit}_i \in \{0, 1\}$ bitovi u prikazu, za $i = 0, \ldots, n-1$.

Po definiciji, prikaz(B) ima isti zapis bez predznaka, pa su bitovi bit_i baš binarne znamenke broja prikaz(B), tj. vrijedi

$$\mathrm{prikaz}(B) := \mathrm{bit}_{n-1} \cdot 2^{n-1} + \cdots + \mathrm{bit}_1 \cdot 2 + \mathrm{bit}_0.$$

Supstitucijom u "obratnu" vezu odmah dobivamo relacije za B preko bitova u njegovom prikazu s predznakom.

Veza broja i prikaza s predznakom (nastavak)

Opet imamo dva slučaja, ovisno o “predznaku”:

- $B = 0, \ldots, 2^{n-1} - 1$, tj. $B \geq 0 \iff \mathrm{bit}_{n-1} = 0$ i tada je

$$
\begin{aligned}
B &= (0 \cdot 2^{n-1}) + \mathrm{bit}_{n-2} \cdot 2^{n-2} + \cdots + \mathrm{bit}_1 \cdot 2 + \mathrm{bit}_0 \\
&= \mathrm{bit}_{n-2} \cdot 2^{n-2} + \cdots + \mathrm{bit}_1 \cdot 2 + \mathrm{bit}_0,
\end{aligned}
$$

- $B = -1, \ldots, -2^{n-1}$, tj. $B < 0 \iff \mathrm{bit}_{n-1} = 1$ i tada je

$$
\begin{aligned}
B &= (1 \cdot 2^{n-1} + \mathrm{bit}_{n-2} \cdot 2^{n-2} + \cdots + \mathrm{bit}_1 \cdot 2 + \mathrm{bit}_0) - 2^n \\
&= (\mathrm{bit}_{n-2} \cdot 2^{n-2} + \cdots + \mathrm{bit}_1 \cdot 2 + \mathrm{bit}_0) - 2^{n-1}.
\end{aligned}
$$

Za negativne B, bitovi bit_i nisu binarne znamenke od B.

Komplement bita

Sad ćemo izvesti jedno jednostavno pravilo o prikazu koje vrijedi (u istom obliku) za sve prikazive brojeve.

Prvo moramo uvesti pojmove komplementa jednog bita i komplementa broja (bez predznaka).

Definicija. Komplement bita (binarne znamenke) $b \in \{0, 1\}$, u oznaci $\bar{b}$, definiramo ovako:

$$\bar{b} := 1 - b.$$

Odmah vidimo da je

$$\bar{0} = 1, \quad \bar{1} = 0,$$

pa je operacija komplement aritmetički ekvivalent negacije.

Komplement broja bez predznaka

Definicija. Komplement prikazivog cijelog broja $B' \in \mathbb{Z}_{2^n}$ (bez predznaka) na n bitova definiramo ovako:

- nađemo prikaz broja B', tj. svih n bitova u prikazu,

$$[\, b_{n-1} \; b_{n-2} \; \ldots \; b_1 \; b_0 \,],$$

- komplementiramo svaki bit u prikazu, $b'_i \mapsto \bar{b}'_i$,

$$[\, \bar{b}_{n-1} \; \bar{b}_{n-2} \; \ldots \; \bar{b}_1 \; \bar{b}_0 \,],$$

- očitamo broj $\bar{B}$ čiji je to prikaz.

Ovo možemo definirati i za brojeve s predznakom, ali nam neće trebati (da ne stvara zabunu).

Komplement broja bez predznaka (nastavak)

Dakle, ako je $B' \in \mathbb{Z}_{2^n}$ oblika

$$B' = b'_{n-1} \cdot 2^{n-1} + b'_{n-2} \cdot 2^{n-2} + \cdots + b'_1 \cdot 2 + b'_0,$$

onda je, očito, $\bar{B}' \in \mathbb{Z}_{2^n}$ i vrijedi

$$\bar{B}' = \bar{b}'_{n-1} \cdot 2^{n-1} + \bar{b}'_{n-2} \cdot 2^{n-2} + \cdots + \bar{b}'_1 \cdot 2 + \bar{b}'_0,$$

Uočimo da za svaki bit vrijedi $b + \bar{b} = 1$ i zbrojimo ove dvije relacije. Dobivamo

$$\begin{aligned} B' + \bar{B}' &= 1 \cdot 2^{n-1} + 1 \cdot 2^{n-2} + \cdots + 1 \cdot 2 + 1 \cdot 1 \\ &= 2^{n-1} + 2^{n-2} + \cdots + 2 + 1 \\ &= 2^n - 1. \end{aligned}$$

Prikaz suprotnog broja preko komplementa

Prebacimo 1 s desne na lijevu stranu

$$B' + \bar{B}' + 1 = 2^n,$$

i zapišimo ovu relaciju "modularnim zbrajanjem" $\oplus_{2^n}$ u $\mathbb{Z}_{2^n}$

$$B' \oplus_{2^n} (\bar{B}' \oplus_{2^n} 1) = 0.$$

Dakle, jedinstveni suprotni element (inverz obzirom na zbrajanje) elementa $B' \in \mathbb{Z}_{2^n}$ jednak je $\bar{B}' \oplus_{2^n} 1$.

Drugim riječima, suprotni broj dobivamo tako da

- komplementiramo broj (odnosno, njegov prikaz) i
- dodamo 1 modulo 2^n.

Prikaz suprotnog broja preko komplementa

Napomena. Modularno dodavanje jedinice služi samo za $B' = 0$. Tada je $\bar{B}' = 2^n - 1$ i moramo dodati 1 modularno, da opet dobijemo 0 kao suprotni element.

Za $B' \in \mathbb{Z}_{2^n}$ i $B' > 0$, suprotni element je $\bar{B}' + 1$.

Potpuno isto "pravilo" vrijedi i za brojeve s predznakom!

Prisjetimo se da je prikaz negativnih brojeva iz $\mathbb{Z}_{2^n}^-$ "podešen" tako da modularna aritmetika radi korektno.

To znači da za svaki $B \in \mathbb{Z}_{2^n}^-$ vrijedi

$$\text{prikaz}(B) \oplus_{2^n} \text{prikaz}(-B) = 0.$$

Ovdje $-B$ treba smatrati suprotnim elementom od B u $\mathbb{Z}_{2^n}^-$.

Prikaz suprotnog broja preko komplementa

Znamo da je $\text{prikaz}(B) = B'$, za neki $B' \in \mathbb{Z}_{2^n}$, pa mora biti

$$\text{prikaz}(-B) = \bar{B}' \oplus_{2^n} 1,$$

zbog jedinstvenosti suprotnog elementa u $\mathbb{Z}_{2^n}$

Opet, prikaz suprotnog broja $\text{prikaz}(-B)$ dobivamo tako da

- komplementiramo prikaz samog broja $\text{prikaz}(B) = B'$ i
- dodamo 1 modulo 2^n.

Ovaj zaključak je direktna posljedica modularne aritmetike u $\mathbb{Z}_{2^n}^-$ i ne ovisi o tome koji broj $B' \in \mathbb{Z}_{2^n}$ izaberemo za prikaz zadanog broja $B \in \mathbb{Z}_{2^n}^-$. Zato i treba dodatno fiksirati prikaz barem jednog broja iz $\mathbb{Z}_{2^n}^-$ (na primjer, $B = 0$) da dobijemo jedinstvenost prikaza.

Dijeljenje cijelih brojeva s predznakom

Prošli puta smo uveli operacije div (cjelobrojni kvocijent) i mod (ostatak) na skupu $\mathbb{Z} \times \mathbb{N}$.

Definicija. Neka su $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ bilo koji brojevi, i neka su $q \in \mathbb{Z}$ (cjelobrojni kvocijent) i $r \in \mathbb{Z}_b$ (ostatak) jedinstveni brojevi za koje vrijedi

$$a = q \cdot b + r.$$

Operacije div i mod definiramo relacijama

$$a \operatorname{div} b := q \in \mathbb{Z}, \quad a \bmod b := r \in \mathbb{Z}_b.$$

Za početak, uočite da su obje operacije definirane na skupu $\mathbb{Z} \times \mathbb{N}$, a kodomene su različite.

Dijeljenje cijelih brojeva s predznakom

Sad nam treba proširenje na skup $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$,

- kad cjelobrojno dijelimo dva cijela broja (što, naravno, ima smisla),

da dobijemo cjelobrojno dijeljenje za cijele brojeve s predznakom $\mathbb{Z}_{2^n}^{-}$ (koji modeliraju $\mathbb{Z}$).

Naravno, ideja je ista kao i kod brojeva bez predznaka.

Cjelobrojno dijeljenje ili dijeljenje s ostatkom cijelih brojeva s predznakom je naprosto

- restrikcija odgovarajućih operacija div i mod.

Dakle, treba nam proširenje tih operacija na $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

Međutim, ne postoji dogovoreni standard za to proširenje.

Dijeljenje cijelih brojeva s predznakom

U većini programskih jezika (uključivo i C) vrijedi da

- stvar radi očekivano (prema Euklidovom teoremu) samo na skupu $\mathbb{N}_0 \times \mathbb{N}$.

Dakle, za nenegativne brojeve s predznakom dobivamo očekivane (i korektne) rezultate u cjelobrojnom dijeljenju.

A za negativne operande? Nije precizno definirano!

Na primjer, C standard (knjiga Kernighan, Ritchie) kaže:

- ako je barem jedan od dva operanda negativan, rezultat ovisi o implementaciji.

Dakle, nije predvidiv — isti program može davati različite rezultate, ovisno o računalu i izboru C compilera.
Zato — čitajte upute ili, naprosto, probajte!

Dijeljenje cijelih brojeva s predznakom

Eksperiment:

- test–program `divmod.c` (pokaži!),
- Intelov C++ compiler (verzija 9.0.025), na IA–32.

Rezultati $q = a \,\mathrm{div}\, b$ i $r = a \bmod b$ za $a = \pm 5$, $b = \pm 3$:

a	b	q	r
5	3	1	2
-5	3	-1	-2
5	-3	-1	2
-5	-3	1	-2

Operacije div i mod interpretiramo na $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

Veza cjelobrojnog i običnog dijeljenja

Ključ za interpretaciju:

- kvocijent se uvijek "zaokružuje" prema nuli,

$$q = \mathrm{sign}\left(\frac{a}{b}\right) \cdot \left\lfloor \left|\frac{a}{b}\right| \right\rfloor,$$

- ostatak ima isti predznak kao i a.

$$r = \mathrm{sign}(a) \cdot (|a| \bmod |b|).$$

Za ostatak r ovdje vrijedi:

- $0 \leq r < |b|$, za $a \geq 0$,
- $-|b| < r \leq 0$, za $a < 0$.

Veza cjelobrojnog i običnog dijeljenja

Razlog: standardno ograničenje na ostatak $0 \le r < b$, tj. $r \in \mathbb{Z}_b$, odgovara cijelim brojevima bez predznaka.

Međutim, kod brojeva s predznakom imamo i negativne brojeve, pa (možda) ima smisla dozvoliti da i ostaci budu negativni (u nekim slučajevima).

Prednosti ovakve "definicije" operacija div i mod na skupu $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$:

- bez obzira na predznake od a i b,
- dobivamo iste apsolutne vrijednosti kvocijenta q i ostatka r,

tj. samo predznaci od q i r ovise o predznacima od a i b.

Ovo je i najčešća realizacija cjelobrojnog dijeljenja u praksi.

Cijeli brojevi s predznakom — sažetak

Ako imamo n bitova za prikaz brojeva, onda je skup svih prikazivih cijelih brojeva bez predznaka jednak

$$\mathbb{Z}_{2^n}^- = \{\, -2^{n-1},\ -2^{n-1}+1,\ \ldots\ ,-1,\\ 0,\ 1,\ \ldots\ ,\ 2^{n-1}-2,\ 2^{n-1}-1 \,\}.$$

Za prikaz broja $B \in \mathbb{Z}_{2^n}^-$ vrijedi:

- nenegativni brojevi $B = 0, \ldots, 2^{n-1}-1$ imaju isti prikaz kao i bez predznaka,
- negativni brojevi $B = -1, \ldots, -2^{n-1}$ imaju isti prikaz kao i brojevi $2^n + B$ bez predznaka.

Cijeli brojevi s predznakom — sažetak

Osim toga, prikaz suprotnog broja $-B$ dobivamo tako da

- komplementiramo prikaz samog broja i dodamo 1 modulo 2^n.

Aritmetika cijelih brojeva s predznakom je modularna aritmetika modulo 2^n na sustavu ostataka $\mathbb{Z}_{2^n}^-$.

- To vrijedi za operacije $+$, $-$ i $\cdot$.

Operacije cjelobrojnog dijeljenja s ostatkom div i mod daju iste rezultate kao da dijelimo u $\mathbb{Z}$,

- ali treba provjeriti kako se dobiva proširenje ovih operacija s $\mathbb{N}_0 \times \mathbb{N}$ na $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

Cijeli brojevi — klasične greške

Primjer. Računanje $n!$ u cjelobrojnoj aritmetici. (Pokaži!)