Treća zadaća iz Teorije, metodike i povijesti infinitezimalnih računa

Filip Nikšić
fniksic@gmail.com

17. veljače 2011.

1. Proučiti hiperproste brojeve i pitanje faktorizacije. Vrijedi li osnovni teorem aritmetike?

Rješenje. Za početak nekoliko konvencija. Sve varijable koje koristimo odnosit će se na cijele (i hipercijele) brojeve. Relacijskim simbolom P označit ćemo proste brojeve (pozitivne i negativne). Po uzoru na Donalda Knutha uvodimo i neuobičajene oznake za djeljivost i relativnu prostost: $a \setminus b$ znači da a dijeli b, a $a \perp b$ znači da su brojevi a i b relativno prosti.

Za pripremu terena, uočimo da su svi aksiomi komutativnog prstena s jedinicom bez djelitelja nule (dakle, integralne domene) rečenice prvog reda, stoga ih možemo transferirati iz $\mathbb{R}$ u $\mathbb{HR}$ i obratno. Nadalje, sljedeća rečenica je istinita u $\mathbb{R}$ pa stoga i u $\mathbb{HR}$:

$$\forall p\Big(P(p) \leftrightarrow (p \neq 0 \wedge p \neq 1 \wedge p \neq -1 \wedge \forall a \forall b(p \setminus ab \rightarrow p \setminus a \vee p \setminus b))\Big)\,.$$

Iz svega ovoga zaključujemo da su hipercijeli brojevi, kao i cijeli, jedna integralna domena te da su u njoj hiperprosti brojevi prosti elementi u uobičajenom smislu.

Lako se vidi da hipercijeli brojevi nisu domena jedinstvene faktorizacije. Naime, fokusirajmo se na uobičajen model za hiperrealne brojeve (ultrapotenciju $\mathbb{R}$ u odnosu na prebrojivo nepotpun ultrafiltar nad $\mathbb{N}$). Promotrimo sljedeći hipercijeli broj:

$$n = (1!, 2!, 3!, 4!, \ldots, k!, \ldots)\,.$$

Očito svaki konačan cijeli broj (izuzev 0) dijeli n pa specijalno i svaki konačan prosti broj. Prema tome, n nema konačan rastav na proste faktore. Zaključak je da osnovni teorem aritmetike ne vrijedi za hipercijele brojeve, a posljedica toga je da se osnovni teorem aritmetike ne može zapisati kao rečenica u jeziku prvog reda.

Glavni razlog zbog koje nam osnovni teorem aritmetike „propada" na hipercijelim brojevima je zahtjev konačnosti rastava. Ako taj zahtjev ispustimo, onda ipak možemo govoriti o nekom obliku jedinstvene faktorizacije. To je zapravo sasvim očekivano: dobili smo beskonačne brojeve pa su s njima došli i beskonačni rastavi.

Da bismo pojasnili što znači „neki oblik jedinstvene beskonačne faktorizacije", označimo s $(p_k)_{k\geqslant 0}$ niz svih konačnih pozitivnih prostih brojeva u rastućem poretku. Tada cijeli broj n različit od 0 ima jedinstveni rastav:

$$n = \operatorname{sgn} n \prod_{k \geqslant 0} p_k^{a_k}\,.$$

Definirajmo $a(n, k) := a_k$. Tada je u $\mathbb{R}$ i $\mathbb{HR}$ istinita rečenica:

$$\forall n\Big(n \neq 0 \rightarrow \forall k(k \geqslant 0 \rightarrow p_k^{a(n,k)} \setminus n \wedge \forall b(b > a(n,k) \rightarrow p_k^b \not\setminus n))\Big)\,.$$

Funkciju $a(n,\cdot)$ možemo identificirati s rastavom broja n.

Proširenje funkcije a na hipercijele brojeve možemo smatrati rastavom beskonačnih hipercijelih brojeva. Ako bi b bila neka druga funkcija koja proširuje a, ona bi bila jednaka a jer je na $\mathbb{R}$ istinita rečenica:

$$\forall n\Big(n \neq 0 \to \forall k(k \geqslant 0 \to a(n,k) = b(n,k))\Big)\,.$$

U tom smislu hipercijeli brojevi imaju jedinstvene rastave na proste faktore.

Pokažimo sada nekoliko primjera hipercijelih brojeva i njihovih rastava u konkretnom modelu.

Primjer 1. $n = (p_0, p_0p_1, \ldots, p_0p_1\cdots p_k, \ldots)$

Očito svaki konačan prosti broj dijeli n s potencijom 1. Dakle, $a(n,k) = 1$ za konačan k. No, što je s beskonačnim k? Primjerice, za $k = (0,1,2,\ldots)$ je $p_k = (p_0, p_1, p_2, \ldots)$ pa vrijedi $p_k \setminus n$. Dakle, $a(n,k) = 1$. No, za $k = (1,2,3,\ldots)$ je $p_k = (p_1, p_2, p_3, \ldots)$ pa vidimo da vrijedi $p_k \not\setminus n$. Stoga $a(n,p_k) = 0$.

Primjer 2. $n = (0!, 1!, 2!, \ldots, k!, \ldots)$

U ovom slučaju vrijedi sljedeća formula za konačan k:

$$a(n,k) = \Big(\lfloor 0/p_k\rfloor + \lfloor 0/p_k^2\rfloor + \ldots, \lfloor 1/p_k\rfloor + \lfloor 1/p_k^2\rfloor + \ldots,\ \ldots, \lfloor i/p_k\rfloor + \lfloor i/p_k^2\rfloor + \ldots,\ \ldots\Big)\,.$$

Dakle, primjerice

$$a(n,0) = (0,0,1,1,3,3,4,4,7,7,\ldots)\,,$$
$$a(n,1) = (0,0,0,1,1,1,2,2,2,5,\ldots)\,.$$

Primjer 3. $n = (2^0, 2^1, \ldots, 2^k, \ldots)$

Vidimo da je $a(n,0) = (0,1,2,\ldots)$ jer je $p_0 = 2$. Za bilo koji drugi konačan k je $a(n,k) = 0$. Što je s beskonačnim k? Postoji li neki beskonačan hiperprosti broj koji dijeli n? Nije teško vidjeti da je odgovor negativan. Drugim riječima, u ovom slučaju n ima konačnu faktorizaciju:

$$n = 2^{(0,1,2,\ldots)}\,.$$

Zanimljivo je razmotriti i poopćenje pojma Euklidove domene. Naime, cijeli brojevi su jedna Euklidova domena, što znači da postoji funkcija $\varphi\colon \mathbb{Z}\backslash\{0\} \to \mathbb{N}$ sa svojstvima:

(1) $ab \neq 0$ povlači $\varphi(a) \leqslant \varphi(ab)$.

(2) Za sve a i sve $b \neq 0$ postoje c i d takvi da je $a = bc + d$, i $d = 0$ ili $\varphi(d) < \varphi(b)$.

Jedan od osnovnih rezultata teorije prstena je da je svaka Euklidova domena domena jedinstvene faktorizacije. Stoga hipercijeli brojevi nisu Euklidova domena. Međutim, funkcija φ ima svoje proširenje $\varphi\colon \mathbb{HZ}\backslash\{0\} \to \mathbb{HN}$ sa svojstvima (1) i (2). Problem je, naravno, u tome što joj kodomena nije $\mathbb{N}$, nego $\mathbb{HN}$. Međutim, mogli bismo govoriti o svojevrsnoj „beskonačnoj Euklidovoj domeni”.

Glavno svojstvo Euklidovih domena je da se u njima može provesti Euklidov algoritam za traženje najvećeg zajedničkog djelitelja. I u beskonačnoj Euklidovoj domeni možemo provesti nešto slično – „beskonačan Euklidov algoritam” (koji zasigurno nije Euklidov, a nije ni algoritam (hiperalgoritam?), no zanemarimo te sitnice). Naime, promotrimo funkcije q i r takve da su $q(a,b,k)$ i $r(a,b,k)$ kvocijent, odnosno ostatak u k-tom koraku Euklidovog algoritma za brojeve a i b. Recimo radi određenosti da $r(a,b,k) = 0$ povlači $q(a,b,k+j) = r(a,b,k+j) = 0$ za sve $j > 0$. Tada je istinito u $\mathbb{R}$:

- $\forall a \forall b \Big(ab \neq 0 \rightarrow \exists k (k > 0 \wedge r(a,b,k) = 0 \wedge \forall j (0 < j < k \rightarrow r(a,b,j) \neq 0)) \Big)$

  k iz prethodne rečenice je očito jedinstven pa možemo definirati funkciju $k(a,b)$ – to je broj koraka Euklidovog algoritma za a i b.

- $\forall a \forall b \Big(ab \neq 0 \rightarrow q\big(a,b,k(a,b)\big) = \gcd(a,b) \vee q\big(a,b,k(a,b)\big) = -\gcd(a,b) \Big)$

  Pritom smo s $\gcd(a,b)$ označili (pozitivan) najveći zajednički djelitelj brojeva a i b.

Principom transfera, prethodne rečenice su istinite i u $\mathbb{HR}$. Stoga možemo govoriti o broju koraka Euklidovog algoritma $k(a,b)$ za hipercijele a i b. Naravno, taj broj ne mora biti konačan. Međutim, i u beskonačnom slučaju $q\big(a,b,k(a,b)\big)$ je najveći zajednički djelitelj od a i b i slično. □

2. Dokazati da ne postoji najmanji beskonačan hiperprirodan broj i izvesti zaključak o uređaju na hiperprirodnim brojevima.

Rješenje. Uz relacijski simbol N za relaciju „biti prirodan broj" i konvenciju da je i 0 prirodan broj, na $\mathbb{R}$ je istinita sljedeća rečenica:

$$\forall n (N(n) \wedge n > 0 \rightarrow N(n-1)) \,.$$

Po principu transfera rečenica je istinita i na $\mathbb{HR}$. Specijalno, za beskonačan hiperprirodan broj n je i $n-1$ hiperprirodan. Zbog zatvorenosti konačnih hiperprirodnih brojeva na zbrajanje, $n-1$ mora biti beskonačan. Budući da vrijedi $n-1 < n$ (također po principu transfera), zaključujemo da ne postoji najmanji beskonačan hiperprirodan broj.

Time smo ustanovili da u skupu hiperprirodnih brojeva postoji podskup (beskonačnih hiperprirodnih brojeva) koji nema najmanji element. Slijedi da hiperprirodni brojevi, za razliku od prirodnih, *ne čine* dobro uređen skup. Iz toga proizlazi važan zaključak da se „dobra uređenost" ne može opisati rečenicom u jeziku prvog reda. □

3. Dokazati da za konačne hiperrealne brojeve x, y vrijedi:

$$x \leqslant y \quad \Longrightarrow \quad st(x) \leqslant st(y) \,.$$

Rješenje. Vrijedi $x = st(x) + \varepsilon$ i $y = st(y) + \delta$ za neke ε i δ, infinitezimale ili 0. Iz pretpostavke $x \leqslant y$ onda slijedi

$$st(x) - st(y) \leqslant \delta - \varepsilon \,.$$

Budući da je lijeva strana realan broj, a desna infinitezimal, mora biti

$$st(x) - st(y) \leqslant 0, \text{ tj. } st(x) \leqslant st(y) \,.$$

□

Literatura

[1] J. M. Henle, E. M. Kleinberg, *Infinitesimal Calculus*, Dover, 2003.

[2] H. J. Keisler, *Elementary Calculus: An Infinitesimal Approach*, on-line izdanje, 2010.

[3] A. Robinson, *Non-standard analysis*, Princeton University Press, 1996.