Hilbert tizedik problémája

Csirmaz László

David Hilbert a századforulón a párizsi Nemzetközi Matematikai Kongresszuson 23 problémát sorolt fel, melyek megoldását az eljövendő századtól várta. Ezek közül a tizedik a következő volt: adjunk meg olyan eljárást (algoritmust), amely minden egész együtthatós (többváltozós) polinomról eldönti, van-e a polinomnak nem-negatív egészekből álló gyökrendszere. Ebben a jegyzetben azt mutatjuk meg, hogy Hilbert várakozásával ellentétben ilyen algoritmus nem létezik.

Tekintsünk egy $n+m$-változós, egész együtthatós $p(\overline{x},\overline{y})$ polinomot. Az $\overline{y}$ változókat *paramétereknek* tekintjük, és ezek rögzitése után megnézzük, hogy a polinomnak az $\overline{x}$ változókban van-e nem-negatív egészekből álló megoldása. Álljon R_p pontosan azokból az $\overline{y}$ paraméterekből, melyekre ilyen megoldás létezik. Ezzel R_p egy természetes számok m-eseiből álló halmaz, vagyis egy *reláció* lesz. Az ilyen típusú relációkat *diphantikus relációknak* nevezzük, s ezek vizsgálata vezetett végül is a fenti eredményhez.

Egy természetes számokon értelmezett és természetes számot felvevő függvény *rekurzív*, ha kiszámítható, azaz ha létezik olyan Turing-gép, ami minden inputra megáll és éppen a függvény értékét számítja ki. A rekurzív függvények sok más ekvivalens definíciója közül mi a következőt fogjuk használni.

Definíció *Rekurzív függvények* az $\omega^n \to \omega^m$ függvények legszűkebb részosztálya, mely egyrész tartalmazza a következő függvényeket:

$$\begin{aligned} f(x,y) &= x+y && \text{összeadás} \\ f(x,y) &= x\cdot y && \text{szorzás} \\ f(x_1,\dots,x_n) &= x_i && \text{projekciófüggvények} \\ f(x,y) &= \begin{cases} 1 & \text{ha } x\ge y, \\ 0 & \text{egyébként} \end{cases} && \text{a } \ge \text{ karakterisztikus függvénye} \end{aligned}$$

másrészt zárt a kompozícióra és a μ-operációra, azaz ha $f(\overline{x},u)$ egy $(n+1)$-változós rekurzív függvény úgy hogy minden $\overline{x}$-hez van olyan u amivel $f(\overline{x},u)=0$, akkor

$$g(\overline{x}) = \mu u(f(\overline{x},u)=0) \stackrel{\text{def}}{=} \min\{u\in\omega \,:\, f(\overline{x},u)=0\}$$

szintén rekurzív.

Csakúgy mint itt, a későbbiekben is ω jelöli a természetes számok halmazát. Egy ω^n-en értelmezett R reláció rekurzív, ha karakterisztikus függvénye, azaz $\chi_R(\overline{x})=1$ ha $\overline{x}\in R$ és $\chi_R(\overline{x})=0$ ha $\overline{x}\notin R$, rekurzív. R *rekurzívan felsorolható*, ha R éppen egy rekurzív függvény értékkészlete. Megjegyezzük, hogy minden rekurzív reláció egyúttal rekurzívan felsorolható is, de fordítva nem: van ω-nak rekurzívan felsorolható, de nem rekurzív részhalmaza.

Egy függvény *parciálisan rekurzív*, ha értelmezési tartománya ω^n valamely részhalmaza, és előáll egy rekurzív függvényből a μ-operáció alkalmazásával, ahol is nem követeljük meg, hogy minden $\overline{x}$ inputra létezzen megfelelő u érték.

A nevezetes *Church-tézis* azt mondja ki, hogy minden (elvben) kiszámítható függvény rekurzív. A tézis számos következménye közül az egyik legnevezetesebb, hogy nincs algoritmus (vagyis kiszámítási eljárás), ami minden Turing-gépre megmondaná, hogy az véges sok lépésen belül megáll-e vagy sem (megállási probléma).

Visszatérve Hilbert 10. problémájához, az 50-es évek elejére *Julia Robinson* bizonyította, hogy amennyiben az $f(n,k) = n^k$ kétváltozós függvény diophantikus, akkor minden rekurzív függvény is az. Ebből viszont már következik, hogy a Hibert által keresett algoritmus nem létezik — amit úgy szokás kifejezni, hogy *Hilbert tizedik problémája megoldhatatlan* (lásd 7. Következmény). Annak igazolása, hogy n^k valóban diophantikus, további 20 évet váratott magára, ez *J. Matijasevics* tétele.

A bizonyításhoz elsőként néhány definíciót vezetünk be, majd pár egyszerű állítást igazolunk.

Definíció Az $R \subset \omega^n$ reláció *diophantikus*, ha van olyan $n+m$-változós egész együtthatós $p(\overline{x}, \overline{z})$ polinom, hogy minden $x_1, \ldots, x_n$ nem-negatív egész számra $\overline{x} = \langle x_1, \ldots, x_n \rangle \in R$ akkor és csak akkor, ha vannak olyan nem-negatív egész $z_1, \ldots, z_m$ számok, hogy $p(\overline{x}, \overline{z}) = 0$.

Definíció Az $f : \omega^n \to \omega$ függvény diophantikus, ha az $\{\langle \overline{x}, y \rangle \in \omega^{n+1} : f(\overline{x}) = y\}$ reláció diophantikus.

1. Állítás*Az $=$, $\neq$, $\leq$, $<$ diophantikus relációk, a $+$, $\cdot$,* id *diophantikus függvények.*

Bizonyítás. Az alábbi átírások alkalmazásával:

$$\begin{aligned}
x = y &\quad\Leftrightarrow\quad x - y = 0 \\
x \leq y &\quad\Leftrightarrow\quad (\exists z \geq 0)\, x + z - y = 0 \\
x \neq y &\quad\Leftrightarrow\quad (\exists z \geq 0)\, (x-y)^2 - 1 - z = 0 \\
x < y &\quad\Leftrightarrow\quad (\exists z \geq 0)\, x + z + 1 - y = 0 \\
x + y = z &\quad\Leftrightarrow\quad x + y - z = 0 \\
x \cdot y = z &\quad\Leftrightarrow\quad x \cdot y - z = 0.
\end{aligned}$$

■

2. Állítás*Ha $R_1 \subset \omega^n$ és $R_2 \subset \omega^n$ diophantikus relációk, akkor $R_1 \vee R_2$ $(= R_1 \cup R_1)$ valamint $R_1 \wedge R_2$ $(= R_1 \cap R_2)$ is azok.*

Bizonyítás. Legyen $\overline{x} \in R_1 \Leftrightarrow (\exists \overline{z} \geq 0)\, p(\overline{x}, \overline{z}) = 0$ valamint $\overline{x} \in R_2 \Leftrightarrow (\exists \overline{u} \geq 0)\, q(\overline{x}, \overline{u}) = 0$. Ekkor

$$\begin{aligned}
\overline{x} \in R_1 \cup R_1 &\quad\Leftrightarrow\quad (\exists \overline{z} \geq 0)(\exists \overline{u} \geq 0)\, p(\overline{x}, \overline{z}) \cdot q(\overline{x}, \overline{u}) = 0, \\
\overline{x} \in R_1 \cap R_1 &\quad\Leftrightarrow\quad (\exists \overline{z} \geq 0)(\exists \overline{u} \geq 0)\, p^2(\overline{x}, \overline{z}) + q^2(\overline{x}, \overline{u}) = 0.
\end{aligned}$$

Ezek alapján az állítás közvetlenül adódik. ■

3. Állítás*Ha f_1 és f_2 diophantikus függvények, akkor $f_1 + f_2$, $f_1 \cdot f_2$ és $f_1 \circ f_2$ (kompozíció) is azok.*

Bizonyítás. Definíció szerint $(f_1 + f_2)(\overline{x}) = y \Leftrightarrow \exists y_1 \geq 0 \exists y_2 \geq 0 \Big(f_1(\overline{x}) = y_1 \wedge f_2(\overline{x}) = y_2 \wedge y_1 + y_2 = y \Big)$. A feltétel szerint a zárójelben diophantikus relációk állnak, így azok metszete is diophantikus. Hasonlóan bizonyítható a többi eset is. ■

Világos, hogy minden diophantikus fügvény egyúttal parciálisan rekurzív is, és hogy a diophantikus relációk rekurzívan felsorolhatók. Láttuk, hogy az alapfüggvények, melyekből a (parciálisan) rekurzív függvényeket felépíthetjük, diophantikusak, továbbá hogy a diophantikus függvények köréből az összeg, szorzat és kompozícióképzés nem vezet ki. Így annak igazolásához, hogy minden parciálisan rekurzív függvény egyúttal diophantikus is, elegendő az alábbi tételt igazolnunk:

4. Tétel*Ha az $f : \omega^{n+1} \to \omega$ függvény diophantikus, akkor a $g(\overline{x}) = \mu u(f(\overline{x}, u) = 0)$ szintén diophantikus.*

Mielőtt a tétel bizonyítására rátérnénk, nézzük néhány következményét. Elsőként az előbb megfogalmazott ekvivalenciát mondjuk ki.

5. Következmény*Egy függvény akkor és csak akkor parciálisan rekurzív, ha diophantikus.*

Bizonyítás. A függvény felépítésére vonatkozó indukcióval. ∎

Kleene első normálforma tétele azt mondja ki, hogy minden n-re létezik univerzális rekurzíve felsorolható reláció, azaz olyan $U_n \subset \omega^{n+1}$, hogy minden rekurzív $R \subset \omega^n$-re található olyan $r \in \omega$, hogy $R = \{\overline{x} \in \omega^n : \langle \overline{x}, r \rangle \in U_n\}$.

6. Következmény (Univerzalitási tétel) *Van olyan $p(x, r, \overline{z})$ egész együtthatós polinom, hogy minden rekurzíve felsorolható $R \subset \omega$ relációhoz található $r \in \omega$, hogy $x \in R \Leftrightarrow (\exists \overline{z} \geq 0) p(x, r, \overline{z}) = 0$.*

7. Következmény (Hilbert tizedik porblémájának megoldhatatlansága)*Legyen $p(x, r, \overline{z})$ egy univerzális polinom. Ekkor nem létezik olyan algoritmus, amely minden $r \in \omega$-ra eldöntené, hogy a $p(r, r, \overline{z}) = 0$ diophantikus egyenletnek van-e megoldása a nem-negatív egész számok körében.*

Bizonyítás. Ha mégis volna ilyen algoritmus, akkor a Chuch-tézis értelmében az

$$R = \{r \in \omega : \text{ a } p(r, r, \overline{z}) = 0 \text{ nem oldható meg } \overline{z} \geq 0\text{-val } \}$$

halmaz szintén rekurzív volna, így a p univerzalitása miatt volna $r \in \omega$, hogy

$$x \in R \quad \Leftrightarrow \quad p(x, r, \overline{z}) = 0 \text{ megoldható } \overline{z}\text{-ben.}$$

Itt $x = r$-et téve kapjuk, hogy

$$p(r, r, \overline{z}) = 0 \text{ megoldható} \quad \Leftrightarrow \quad p(r, r, \overline{z}) = 0 \text{ nem olható meg,}$$

ami nyilván ellentmondás. ∎

Nem nehéz belátni (lásd a feladatokat), hogy van negyedfokú univerzális polinom. Így Hilbert tizedik problémája már negyedfokú polinomokra sem oldható meg. Ugyanakkor ismeretes algoritmus, mely tetszőleges első- és másodfokú polinom esetén megmondja, van-e a polinomnak egész gyöke vagy sem (ez C. L. Siegel 1972-es eredménye). Harmadfokú polinomokra a kérdés nyitva van.

Más oldalról az univerzális polinomok változóinak számát vizsgálhatjuk. Jól ismert, hogy egy egyváltozós egész együtthatós polinom egész gyöke (ha van) osztója a konstans tagnak, így egyváltozós polinomokra is létezik eldöntő algoritmus. J. Robinson és J. Matijasevics konstruált 13 ismeretlenes univerzális polinomot, ennek fokszáma azonban igen magas, nagyobb mint $10^{10^{10}}$. A következő fokszám–változószám párok mellett ismert univerzális polinom: (4,153), (6,129), (8,108), (10,107), (20,86), (44,83), (1952,80). Az ismert legkisebb lehetséges változószám kilenc: 9-változós polinomok olyan sorozatát lehet megadni, melyekre nem létezik eldöntő algoritmus. A hiányzó $2, 3, \ldots, 8$ esetekre szinte semmi sem ismert.

Az univerzális polinom létezésének egyik meglepő következménye, hogy elegendően nagy q-ra (például $q \geq 14$ megteszi) a legalább q tényezős szorzatra felbontható számok halmaza, vagyis az

$$\{x \in \omega : \exists z_1 \geq 0 \ldots \exists z_q \geq 0 \; x = (z_1+2)\cdot(z_2+2)\cdot \cdots \cdot(z_q+2)\}$$

reláció definiálható q-nál kevesebb paraméterrel is.

Az 5. következmény bizonyítása – könnyen látható módon – formalizálható a Peano axiómarendszerben. Mivel egy reláció akkor és csak akkor rekurzíve felsorolható, ha van azt definiáló Σ_1 formula, azonnal adódik az alábbi

8. Következmény *Minden $\varphi(\overline{x})$ Σ_1 Peano formulához található olyan $\psi(\overline{x}, \overline{z})$ kvantormentes (prím) formula, hogy $PA \vdash \varphi(\overline{x}) \leftrightarrow \exists z_1 \ldots \exists z_m \psi(\overline{x}, \overline{z})$.*

Más szavakkal a Σ_1 formulák ekvivalensek az ún. egzisztenciális formulákkal, melyekben egyátalán nem szerepel korlátos kvantor. Az aritmetikai hierarchia felépítésében így a Σ_n, Π_n formulákban $n \geq 1$-re feltehetjük, hogy nem szerepel korlátos kvantor.

Most rátérünk a 4. tétel bizonyítására. Legyen tehát a $p(\overline{x}, u, y, \overline{z})$ egész együtthatós polinom olyan, hogy minden $\overline{x} \in \omega^n$, $u, y \in \omega$ mellett

$$f(\overline{x}, u) = y \text{ akkor és csak akkor, ha } (\exists \overline{z} \geq 0) p(\overline{x}, u, y, \overline{z}) = 0.$$

Legyen $g(\overline{x}) = \mu u(f(\overline{x}, u) = 0)$. A μ operáció definíciója alapján adott $\overline{x} \in \omega^n$ és $u \in \omega$ esetén $g(\overline{x}) = u$ pontosan akkor áll fenn, ha $f(\overline{x}, u) = 0$, továbbá minden $0 \leq v < u$ esetén $f(\overline{x}, v)$ definiálva van és 0-tól különböző, azaz értéke $y+1$ valamilyen $y \geq 0$-ra. Így $g(\overline{x}) = u$ pontosan akkor, ha

$$(\exists \overline{z} \geq 0) p(\overline{x}, u, 0, \overline{z}) = 0 \wedge (\forall v < u)(\exists \overline{z} \geq 0)(\exists y \geq 0) p(\overline{x}, v, y+1, \overline{z}) = 0.$$

Ahhoz, hogy g valóban diophantikus függvény legyen, elegendő az itt szereplő diszjunkció második tagjáról megmutatni, hogy diophantikus reláció. A jelölések egyszerűsítése érdekében az y változót a $\overline{z}$ paraméterek közé soroljuk, és a szereplő (most már) $n+1+m$-változós polinomot P-vel jelöljük. Így azt kell igazolnunk, hogy a következő $n+1$-változós reláció diophantikus:

$$R = \{\langle \overline{x}, u \rangle \in \omega^{n+1} : (\forall v < u)(\exists \overline{z} \geq 0) P(\overline{x}, v, \overline{z}) = 0\}.$$

Legyen $\langle \overline{x}, u \rangle \in R$ tetszőleges de rögzített. Ekkor persze minden $0 \leq v < u$-hoz van olyan $\overline{z} \in \omega^m$, melyre $P(\overline{x}, v, \overline{z}) = 0$, jelöljük az egyik ilyet $\overline{z}^{(v)}$-vel, és legyen z az összes $\overline{z}^{(v)}$-ben szereplő természetes szám mindegyikénél nagyobb. Vegyük ω^m-nek mindazokat a $\overline{t}$ elemeit, melyekre $\overline{t} < z$, azaz $\overline{t}$-nak mind az m eleme kisebb z-nél, és legyen M olyan nagy, hogy $v < u$ és $\overline{t} < z$ esetén

$$\left| P(\overline{x}, v, \overline{t}) \right| < M,$$

továbbá $u < M$ és $z < M$ is teljesül.

Ha most $b_0, b_1, \ldots, b_{u-1}$ páronként relatív prím, M-nél nagyobb egész, akkor a kínai maradéktétel értelmében van olyan $c > 0$ egész, melyre

$$c \equiv v \pmod{b_v} \quad v = 0, 1, \ldots, u-1.$$

Továbbá ha $\overline{z}^{(v)}$ elemeit $z_1^{(v)}$, $z_2^{(v)}$, …, $z_m^{(v)}$ jelöli, akkor vannak olyan a_1, …, a_m pozitív számok is, hogy

$$a_1 \equiv z_1^{(v)} \pmod{b_v} \qquad v = 0, 1, \dots, u-1$$
$$\dots$$
$$a_m \equiv z_m^{(v)} \pmod{b_v} \qquad v = 0, 1, \dots, u-1.$$

Ekkor természetesen $P(\overline{x}, c, \overline{a}) \equiv P(\overline{x}, v, \overline{z}^{(v)}) = 0 \pmod{b_v}$, ahol $\overline{a} = \langle a_1, \dots, a_m \rangle$, tehát a $b_0 \cdot b_1 \cdot \ldots \cdot b_{u-1}$ szorzatot s-sel jelölve

$$P(\overline{x}, c, \overline{a}) \equiv 0 \pmod{s}.$$

Az $a_j - z_j^{(v)}$ különbség osztható b_v-vel, a $z_1(v)$, …, $z_m^{(v)}$ mindegyike kisebb z-nél, ezért a $\prod_{i<z}(a_j - i)$ szorzat osztható a relatív prím b_v-k szorzatával, s-sel is. Ezzel igazoltuk a következő lemma első felét:

9. Lemma$\langle \overline{x}, u \rangle \in R$ *akkor és csak akkor, ha vannak olyan M, z, s, c és a_1, …, a_m nem-negatív egészek, melyekre*

(i) *minden $v < u$ és $\overline{t} < z$ esetén $\left|P(\overline{x}, v, \overline{t})\right| < M$, továbbá $2u + 3 < M$ és $z < M$;*

(ii) *s felbontható u darab páronként relatív prím szám, b_0, …, b_{u-1} szorzatára úgy, hogy mindegyik tényezőnek van M-nél nagyobb prímosztója, továbbá minden $v < u$-ra $c \equiv v \pmod{b_v}$;*

(iii) *minden $j = 1, \dots, m$-re $\prod_{i<z}(a_j - i)$ osztható s-sel;*

(iv) *$P(\overline{x}, c, \overline{a}) \equiv 0 \pmod{s}$.*

Bizonyítás. A fentebb mondottak értelmében elegendő a megfordítást igazolni. Legyen $0 \leq v < u$ esetén p_v a b_v-nek M-nél nagyobb ((ii) szerint létező) prímosztója, és $j = 1, 2, \dots, m$-re $z_j^{(v)}$ éppen a_j-nek p_v-vel való osztásakor adódó maradék, végül $\overline{z}^{(v)} = \langle z_1^{(v)}, \dots, z_m^{(v)} \rangle$. Ekkor (iv) alapján

$$P(\overline{x}, v, \overline{z}^{(v)}) \equiv 0 \pmod{p_v}$$

hiszen p_v osztója s-nek és $c \equiv v \pmod{b_v}$, ezért ez a kongruencia mod p_v is fennáll. (iii) szerint $\prod_{i<z}(a_j - i)$ osztható b_v-vel, ezért p_v-vel is, tehát a_j-nek p_v-vel való osztásakor a maradék csak 0, 1, …, $z - 1$ közül kerülhet ki, vagyis $z_j^{(v)} < z$. Így (i) miatt

$$\left|P(\overline{x}, v, \overline{z}^{(v)})\right| < M < p_v,$$

következésképp $P(\overline{x}, v, \overline{z}^{(v)})$ értéke csak nulla lehet.

Minden $v < u$-ra találtunk tehát olyan $\overline{z} \geq 0$-t, amire $P(\overline{x}, v, \overline{z}) = 0$, így $(\overline{x}, u) \in R$, ahogyan kívántuk. ∎

Könnyű olyan $Q(\overline{x}, u, z)$ polinomot találni, hogy adott $\overline{x} \in \omega^n$, u, $z \in \omega$ mellett minden $0 \leq v < u$ és $\overline{t} \in \omega^n$, $\overline{t} < z$ esetén

$$\left|P(\overline{x}, v, \overline{t})\right| \leq Q(\overline{x}, u, z)$$

legyen. Egyszerűen P-ben az összes együtthatót az abszolút értékével helyettesítjük, továbbá az utolsó m darab z_1, …, z_m változó mindegyikének a helyébe z-t írunk. Ekkor a lemma (i) feltétele az $M = Q(\overline{x}, u, z) + 2u + z + 1$ választással nyilván teljesül. (iv)-ről könyen látható, hogy diophantikus reláció, így elegendő (ii)-vel és (iii)-vel foglalkoznunk.

Az, hogy az (iii) alatti m darab reláció mindegyike diophantikus, azonnal következik abból, hogy az $f(x) = x!$ faktoriális függvény diophantikus. Valóban, $\prod_{i<z}(a-i)$ pontosan akkor osztható s-sel, ha (az (i) és (ii) szerint) pozitív tényezőkből álló

$$\prod_{i<z}(a+s-i) = \frac{(a+s)!}{(a+s-z)!}$$

szorzat osztható s-sel, azaz ha van olyan $q_a \geq 0$ egész, hogy

$$(a+s)! = q_a \cdot s \cdot (a+s-z)!.$$

Ez valóban diophantikus, ha $x!$ az.

Végül (ii)-ben s-et és c-t is meg tudjuk diophantikus függvénnyel adni, ugyanilyen feltétel mellett. A

$$b_v = \frac{M!-v-1}{v+1} \qquad v = 0, \ldots, u-1$$

választással ugyanis a b_v-k szorzata

$$s = \frac{M!-1}{1} \cdot \frac{M!-2}{2} \cdot \ldots \cdot \frac{M!-u}{u} = \binom{M!-1}{u} = \frac{(M!-1)!}{u!(M!-1-u)!}$$

és még $b_{u-1} > M$ is teljesül, ha $M > u+3$. Ha pedig

$$c = M! - 1$$

akkor $c - v = M! - 1 - v$ valóban osztható b_v-vel. Így csak azt kell ellenőriznünk, hogy a b_v számok páronként relatív prímek, és mindegyiknek van M-nél nagyobb prímosztója. Legyen $0 \leq i < j < u$. Ha egy p prímszám osztója lenne b_i-nek és b_j-nek, akkor

$$p \mid b_i - b_j = \frac{M!(j-i)}{ij},$$

tehát $M > u > j - i$ miatt p mindenképpen osztója lenne $M!$-nak is. Ezért $p \mid b_i = \frac{M!}{i+1} - 1$ csak úgy lehet, ha p egyúttal $(i+1)$-nek is osztója. De $i+1 \leq u$ és $2u < M$ esetén p biztosan osztója lesz $\frac{M!}{i+1}$-nek, tehát nem lehet osztója az ennél eggyel kisebb számnak, b_i-nek.

A fenti okoskodás egyúttal azt is adja, hogy b_i-nek egyátalán nincs M-nél kisebb prímosztója, tehát p_i-nek b_i tetszőleges prímosztója megfelelő.

10. Lemma*Ha az $f(x) = x!$ függvény diophantikus, akkor az R reláció is az.*

Bizonyítás. Az előzőek alapján $\langle \overline{x}, u \rangle \in R$ akkor és csak akkor, ha vannak olyan M, z, x, $c \in \omega$ és $\overline{a} \in \omega^m$ egészek, melyekre

(i) $M = Q(\overline{x}, u, z) + 2u + z + 4$;

(ii) $s = \binom{M!-1}{u} = \frac{(M!-1)!}{u!(M!-1-u)!}, \quad c = M! - 1$;

(iii) minden $j = 1, 2, \ldots, m$-re $s \,\Big|\, \frac{(a_j+s)!}{(a_j+s-z)!}$;

(iv) $P(\overline{x}, c, \overline{a}) \equiv 0 \pmod{s}$.

Mivel ezen relációk mindegyike diophantikus a mondott feltétel mellett, a lemma állítását beláttuk. ∎

Ezek után elegendő egyetlen függvényről, nevezetesen az $x!$ függvényről igazolnuk, hogy diophantikus, ebből már következik, hogy minden parciálisan rekurzív függvény is az. Ehhez először igazoljuk, hogy ha a $g(x,y) = x^y$ hatványfüggvény diophantikus, akkor a faktoriális függvény is az, majd egy speciális típusú Pell-egyenlet vizsgálata után a hatványfüggvényről is belátjuk, hogy diophantikus.

11. Lemma*Ha a hatványfüggvény diophantikus, akkor a faktoriális függvény is az.*

Bizonyítás. Állítjuk, hogy $y = k!$ akkor és csak akkor, ha vagy $k = 0$ és $y = 1$, vagy ha vannak olyan n, u, a és $b \in \omega$ értékek, hogy

$$k \geq 1,\ n = k^2\cdot(2k)^k+1,\ u = 2^n+1;$$

$$a\cdot y \leq n^k < a\cdot(y+1) \qquad (\text{azaz } y = \left[\frac{n^k}{a}\right]);$$

$$b\cdot u^k \leq (u+1)^n < (b+1)\cdot u^k \qquad (\text{azaz } b = \left[\frac{(u+1)^n}{u^k}\right]);$$

$a < u,\ u \mid b - a$ (azaz b-nek u-val való osztásakor adódó maradék éppen a).

Ezek a relációk nyilván mind diophantikusak, ha a $g(x,y) = x^y$ az.

Mivel k értéke egyértelműen meghatározza n-et és az u-t, továbbá ezek b-t, b és u a-t, végül n, k, és a értéke y-t, azért ezeket a feltételeket pontosan egy y elégíti ki. Elegendő tehát megmutatnunk, hogy $y = k!$-ra a feltételek kielégíthetők.

Először is a binomiális tétel alapján

$$\frac{(u+1)^n}{u^k} = \sum_{i>k}\binom{n}{i}u^{i-k} + \binom{n}{k} + \sum_{i<k}\binom{n}{i}u^{i-k}.$$

Az $u = 2^n + 1 > 2^n$ feltételből azonnal adódik, hogy az összeg harmadik tagja 1-nél kisebb, az első szumma mindegyik tagja osztható u-val és $u > 2^n \geq \binom{n}{k}$, ezért $(u+1)^n/u^k$ egész részét u-val osztva a maradék éppen $\binom{n}{k}$, tehát $a = \binom{n}{k}$. Így elegendő megmutatnunk, hogy $n = k^2\cdot(2k)^k + 1 > k^2\cdot(2k)^k$ esetén

$$k! = \left[\frac{n^k}{\binom{n}{k}}\right].$$

Ennek bizonyításához először megjegyezzük, hogy $0 < \alpha < 1$ és $k \geq 1$ esetén $(1-\alpha)^k \geq 1 - k\cdot\alpha$, tehát

$$\Big(1-\frac{k}{n}\Big)^k \geq 1 - \frac{k^2}{n} > 1 - \frac{1}{(2k)^k} = 1 - \Big(\frac{1}{k} - \frac{1}{2k}\Big)^k > 1 - \Big(\frac{1}{k} - \frac{1}{n}\Big)^k,$$

és így

$$1 < \Big(1-\frac{k}{n}\Big)^k + \Big(\frac{1}{k} - \frac{1}{n}\Big)^k = \Big(1-\frac{k}{n}\Big)^k\Big(1 + \frac{1}{k^k}\Big).$$

Ezek után

$$k! \leq k!\frac{n^k}{n(n-1)\ldots(n-k+1)} = \frac{n^k}{\binom{n}{k}} < k!\Big(\frac{n}{n-k}\Big)^k = k!\frac{1}{\Big(1-\dfrac{k}{n}\Big)^k} < k!\Big(1+\frac{1}{k^k}\Big) \leq k! + 1$$

ahogyan állítottuk. ∎

A hátralevő részben azt bizonyítjuk be, hogy a hatványfüggvény diophantikus. Ezt egy speciális típusú Pell-egyenlet vizsgálatával kezdjük.

Legyen a egynél nagyobb egész, és $d = a^2 - 1$. $(a+\sqrt{d})(a-\sqrt{d}) = 1$ miatt $(a+\sqrt{d})^n = (a-\sqrt{d})^{-n}$, így minden n egész számra egyértelműen találhatók olyan $x_a(n)$ és $y_a(n)$ egész számok, hogy

$$(a+\sqrt{d})^n = x_a(n) + y_a(n)\sqrt{d}, \tag{1}$$

és ekkor persze

$$(a-\sqrt{d})^n = x_a(n) - y_a(n)\sqrt{d}. \tag{2}$$

Speciálisan $x_a(0) = 1$, $y_a(0) = 0$, $x_a(1) = a$, $y_a(1) = 1$, továbbá $n > 0$ esetén $x_a(n)$ és $y_a(n)$ pozitívak, $x_a(n) = x_a(-n)$ valamint $y_a(n) = -y_a(-n)$. Mivel $(a+\sqrt{d})^{n+m} = (a+\sqrt{d})^n \cdot (a+\sqrt{d})^m$, (1)-ből azonnal adódik, hogy

$$\begin{aligned} x_a(n+m) &= x_a(m)x_a(n) + d \cdot y_a(m)y_a(n) \\ y_a(n+m) &= x_a(m)y_a(n) + x_a(n)y_a(m). \end{aligned} \tag{3}$$

Ezeket $m = \pm 1$-re felírva és páronként összeadva

$$\begin{aligned} x_a(n+1) + x_a(n-1) &= 2ax_a(n) \\ y_a(n+1) + y_a(n-1) &= 2ay_a(n), \end{aligned} \tag{4}$$

tehát az $\{x_a(n)\}$ és $\{y_a(n)\}$ sorozatok kielégítik az

$$r_{n+1} = 2ar_n - r_{n-1}$$

rekurziót. (3)-ban $m = 1$-et téve

$$\begin{aligned} x_a(n+1) &= ax_a(n) + dy_a(n) \\ y_a(n+1) &= ay_a(n) + x_a(n) \end{aligned}$$

adódik. Így $n \geq 0$-ra mind $x_a(n)$ mind $y_a(n)$ n-ben szigorúan monoton nő, továbbá $n \geq 1$-re

$$\begin{aligned} \frac{(2a-1)^n}{2} &< x_a(n) \leq \frac{(2a)^n}{2}, \\ (2a-1)^{n-1} &\leq y_a(n) \leq (2a)^{n-1}, \end{aligned} \tag{5}$$

ez szimultán rekurzióval egyszerűen látható.

12. Tétel*Az $x^2 - dy^2 = 1$ Pell-egyenlet nem-negatív megoldásai pontosan az $\langle x_a(n), y_a(n)\rangle$ párok $n \geq 0$-ra.*

Bizonyítás. Az (1) és (2) összefüggéseket összeszorozva

$$x_a(n)^2 - d \cdot y_a(n)^2 = 1,$$

vagyis $\langle x_a(n), y_a(n)\rangle$ valóban megoldás. Legyen most $\langle x, y\rangle$ a Pell egyenletnek ezektől különböző, nem-negatív egészekből álló megoldása, továbbá legyen $n \geq 0$ olyan, hogy

$$(a+\sqrt{d})^n \leq x + y\sqrt{d} < (a+\sqrt{d})^{n+1}.$$

Itt egyenlőség nem állhat, mert akkor $x = x_a(n)$ és $y = y_a(n)$ volna. Legyenek x' és y' olyan egészek, hogy

$$x' + y'\sqrt{d} = \frac{x + y\sqrt{d}}{(a+\sqrt{d})^n} = (x + y\sqrt{d})(a+\sqrt{d})^{-n} = (x + y\sqrt{d})(x_a(n) - y_a(n)\sqrt{d}).$$

Ekkor $1 < x' + y'\sqrt{d} < a + \sqrt{d}$, és könnyen ellenőrizhető, hogy $x'^2 - dy'^2 = 1$. Megmutatjuk, hogy ez lehetetlen. Valóban,

$$(x' + y'\sqrt{d})(x' - y'\sqrt{d}) = 1,$$

és itt mindkét tényező pozitív (hiszen az első még 1-nél is nagyobb), tehát a reciprokokat véve $1 > x' - y'\sqrt{d} > (a+\sqrt{d})^{-1} = a - \sqrt{d}$, azaz

$$-1 < -x' + y'\sqrt{d} < -a + \sqrt{d}.$$

Ezt a fenti $1 < x' + y'\sqrt{d} < a + \sqrt{d}$ egyenlőtlenséghez hozzáadva $0 < 2y'\sqrt{d} < 2\sqrt{d}$, azaz $0 < y' < 1$ adódik, ami lehetetlen, hiszen y' egész. ∎

A továbbiakban a megoldások oszthatósági viszonyait vizsgáljuk. Először is megállapítjuk, hogy $x_a(n)$ és $y_a(n)$ relatív prímek minden n-re, hiszen ha b osztója mindkettőnek, akkor osztója $x_a(n)^2 - dy_a(n)^2 = 1$-nek is, tehát $b = 1$.

13. Lemma$y_a(m) \mid y_a(n)$ *akkor és csak akkor, ha* $m \mid n$.

Bizonyítás. (3) alapján

$$y_a(n-m) = x_a(m)y_a(n) - x_a(n)y_a(m),$$

ezért $y_a(m)$ és $y_a(n)$ legnagyobb közös osztója egyúttal osztója $y_a(n-m)$-nek is. Másrészt $y_a(m)$ és $x_a(m)$ relatív prímek, így az $y_a(n-m)$ és $y_a(m)$ legnagyobb közös osztója osztója $y_a(n)$-nek, tehát

$$\text{lnko}(y_a(m), y_a(n)) = \text{lnko}(y_a(n-m), y_a(n)).$$

Innen az euklídeszi algoritmus alapján $y_a(0) = 0$ miatt

$$\text{lnko}(y_a(m), y_a(n)) = y_a(\text{lnko}(m, n)),$$

amiből a lemma állítása következik. ∎

14. Lemma$y_a(i)^2 \mid y_a(i{\cdot}k)$ *akkor és csak akkor, ha* $y_a(i) \mid k$.

Bizonyítás. Először is megjegyezzük, hogy

$$x_a(i{\cdot}k) + y_a(i{\cdot}k)\sqrt{d} = (a+\sqrt{d})^{i\cdot k} = (x_a(i) + y_a(i)\sqrt{d})^k.$$

Ennek alapján a binomiális tételből

$$y_a(i{\cdot}k) = \binom{k}{1} y_a(i)x_a(i)^{k-1} + \binom{k}{3} d{\cdot}y_a(i)^3 x_a(i)^{k-3} + \dots,$$

és így

$$y_a(i{\cdot}k) \equiv k{\cdot}y_a(i)x_a(i)^{k-1} \pmod{y_a(i)^3}.$$

Innen a lemma "csak akkor" része közvetlenül adódik.

A fordított irányú implikáció bizonyításához tegyük fel, hogy $y_a(i)^2 \mid y_a(i{\cdot}k)$. A fenti kongruencia alapján ekkor $k{\cdot}y_a(i)x_a(i)^{k-1}$ is osztható $y_a(i)^2$-tel, ami $x_a(i)$ és $y_a(i)$ relatív prím volta miatt az jelenti, hogy $y_a(i)$ osztója k-nak. ∎

15. Lemma *Tegyük fel, hogy* $x_a(i) \equiv x_a(j) \pmod{x_a(n)}$. *Ekkor vagy* $i \equiv j \pmod{4n}$, *vagy* $i \equiv -j \pmod{4n}$.

Bizonyítás. A (3) összefüggés szerint

$$x_a(m+n) + x_a(m-n) = 2x_a(n)x_a(m),$$

hiszen $x_a(n) = x_a(-n)$ és $y_a(n) = -y_a(-n)$. Ennek alapján

$$x_a(j) = x_a((j-n)+n) \equiv -x_a((j-n)-n) = -x_a(j-2n) \pmod{x_a(n)},$$

és így

$$x_a(j) \equiv -x_a(j-2n) \equiv x_a(j-4n) \pmod{x_a(n)}.$$

Feltehetjük tehát, hogy $0 \leq i, j < 4n$. Továbbá ugyancsak a fentiek miatt

$$x_a(i) \equiv -x_a(2n-i) \equiv -x_a(2n+i) \equiv x_a(4n-i) \pmod{x_a(n)},$$

továbbá

$$x_a(0) \equiv 1, \quad x_a(n) \equiv 0, \quad x_a(2n) \equiv -1, \quad x_a(3n) \equiv 0 \pmod{x_a(n)}.$$

Ha most még azt is tudjuk, hogy $x_a(n-1) < \frac{1}{2}x_a(n)$, akkor készen vagyunk. Az $x_a(n)$ sorozat ugyanis szigorúan monoton nő $n \geq 0$-ra, és így

$$1 = x_a(0) < x_a(1) < \ldots < x_a(n-1) < \frac{1}{2}x_a(n) < x_a(n) - x_a(n-1) < \ldots < x_a(n) - x_a(0) < x_a(n),$$

tehát az $x_a(0), \ldots, x_a(2n)$ számok mind különböző maradékot adnak $x_a(n)$-nel osztva. Következésképp a $0 \leq j < 4n$ intervallumon az 1-et és -1-et kivéve minden maradék pontosan kétszer fordul elő: egyszer j-re, másszor $4n-j$-re. Így ha $0 \leq i, j < 4n$, továbbá $x_a(i) \equiv x_a(j) \pmod{x_a(n)}$, akkor vagy $i = j$ vagy $i = 4n - j$, ahogyan állítottuk.

A (3) összefüggés szerint

$$x_a(n) = a \cdot x_a(n-1) + d \cdot y_a(n-1),$$

ezért

$$\frac{1}{2}x_a(n) \geq \frac{1}{a}x_a(n) = x_a(n-1) + \frac{d}{a}y_a(n-1) > x_a(n-1),$$

hiszen $n \geq 2$ és ezért $y_a(n-1) > 0$. Ezzel a lemmát beláttuk. ∎

16. Lemma *Legyenek* a, b *egynél nagyobb egészek, és* $a \equiv b \pmod{c}$ *Ekkor* $x_a(n) \equiv x_b(n) \pmod{c}$ *minden* $n \geq 0$*-ra.*

Bizonyítás. Az állítás igazsága $n = 0$-ra és $n = 1$-re közvetlenül ellenőrizhető. Nagyobb n-ekre a (4)-ből adódó

$$x_a(n+1) = 2ax_a(n) - x_a(n-1)$$

rekurzív összefüggés alapján teljes indukcióval bizonyítható. ∎

17. Lemma $y_a(n) \equiv n \pmod{a-1}$.

Bizonyítás. Az $y_a(n+1) = 2ay_a(n) - y_a(n-1) = (2a-2)y_a(n) + 2y_a(n) - y_a(n-1)$ összefüggés alapján teljes inducióval. ∎

18. Tétel*Az $y_a(k)$ kétváltozós függvény diophantikus.*

Bizonyítás. Megmutatjuk, hogy $a \geq 1$ és $k \geq 1$ esetén $y = y_a(k)$ akkor és csak akkor igaz, ha vannak olyan b, u, v, s, t és x nem-negatív egész számok, melyekre a következő tizenegy diophantikus reláció mindegyike teljesül:

(i) $x^2 - (a^2-1)y^2 = 1, \quad u^2 - (a^2-1)v^2 = 1, \quad s^2 - (b^2-1)t^2 = 1;$

(ii) $0 \leq v, \quad k \leq y, \quad 1 < b;$

(iii) $4y \mid b-1, \quad y^2 \mid v;$

(iv) $a \equiv b \pmod{u}, \quad x \equiv s \pmod{u}, \quad t \equiv k \pmod{b-1}.$

Ezzel az állítást nyilván beláttuk, hiszen a hiányzó $a \leq 1$ illetve $k = 0$ esetekben a függvényt könnyű diophantikus relációkkal definiálni.

Elsőként tegyük fel, hogy $y = y_a(k)$, és keressünk olyan b, u, v, a, t és x értékeket, amikre az összes reláció fennáll.

Legyen $n = 2ky_a(k)$, továbbá $x = x_a(k)$, $u = x_a(n)$, $v = y_a(n)$, $a = x_b(k)$, $t = y_b(k)$. Ezekkel a választásokkal (i) mindhárom egyenlőtlensége teljesül. Feltételünk szerint $k \geq 1$, ezért $n \geq 2$, tehát $0 < y_a(n) = v$, és $k = y_a(k) = y$ is teljesül. Mivel $y_a(k) \mid n$, azért a 14. lemma alapján $y_a(k)^2 \mid y_a(n)$, tehát $y^2 \mid v$.

A b-t úgy kell megválasztanunk, hogy egyrészt $b \equiv 1 \pmod{4y}$, másrészt $b \equiv a \pmod{u}$ legyen. Ilyen b biztosan van (mégpedig akármilyen nagy is), ha $4y$ és u relatív prímek. De egyrészt $y_a(n)$ páros, hiszen n páros, és (3) alapján

$$y_a(2m) = 2y_a(m)x_a(m);$$

másrészt $k \mid n$ és így az 13. lemma miatt $y_a(k) \mid y_a(n)$. Ezért $4y = 4y_a(k)$ minden prímosztója osztója $y_a(n)$-nek is, $y_a(n)$ és $x_a(n) = u$ relatív prímek, tehát $4y$-nak és u-nak nincs közös prímosztója — valóban relatív prímek. Miután $b > 1$-et így megválasztottuk, a 16. lemma alapján $x_a(k) \equiv x_b(k) \pmod{u}$, vagyis $x \equiv s \pmod{u}$, amivel (iv) második kongruenciáját is beláttuk. Végül az 17. lemma alapján $t = y_b(k) \equiv k \pmod{b-1}$.

Fordítva, tegyük fel, hogy $a > 1$, $k \geq 1$, és vannak a (i)–(iv) relációkat kielégítő b, u, v, s, t, x és y természetes számok, azt akarjuk belátni, hogy $y = y_a(k)$.

Mivel a, $b > 1$, az $\langle x, y\rangle$, $\langle u, v\rangle$ és $\langle s, t\rangle$ párok megoldásai egy–egy Pell-egyenletnek, tehát vannak olyan i, j és n nem-negatív egészek, hogy

$$x = x_a(i),\, y = y_a(i), \quad u = x_a(n),\, v = y_a(n), \quad s = x_b(j),\, t = y_b(j),$$

és azt szeretnénk belátni, hogy $i = k$. A $k \leq y$ feltétel miatt $y = y_a(i) \neq 0$, így $i > 0$, továbbá $v = y_a(n) > 0$ és ezért $n > 0$ is áll. $y^2 \mid v$, ahonnan $v \neq 0$ miatt $y \leq v$. Ha most $n = 1$, akkor $v = y_a(1) = 1$ és $k \leq y - y_a(i) \leq v$ alapján $k = i = 1$. Így feltehetjük, hogy $n \geq 2$, amikor is $v = y_a(n) > 2$. Ekkor az $y^2 \mid v$ feltételből $y = y_a(i) < v = y_a(n)$, tehát $i < n$.

Tudjuk, hogy $a \equiv b \pmod{u}$, így alkalmazhatjuk a 16. lemmát:

$$x_a(j) \equiv x_b(j) = s \equiv x - x_a(i) \pmod{u}.$$

Most $u = x_a(n)$, $0 < i < n$, tehát a 15. lemma alapján

$$j \equiv \pm i \pmod{4n}$$

valamelyik előjellel. Tudjuk azt is, hogy $y^2 = y_a(i)^2$ osztója $v = y_a(n)$-nek, ezért a 14. lemma szerint $y \mid n$, tehát

$$j \equiv \pm i \pmod{4y}$$

valamilyen előjellel.

Az 17. lemma és (iv) harmadik kongruenciája szerint

$$k \equiv t = y_b(j) \equiv j \pmod{b-1}$$

és mivel $4y \mid b-1$, azért

$$k \equiv j \pmod{4y}.$$

Végül is azt kaptuk, hogy $k \equiv \pm i \pmod{4y}$ valamilyen előjellel, $i \leq y_a(i) = y$, továbbá a (ii) feltétel miatt $k \leq y$, így ez a kongruencia csak úgy állhat fönn, ha $k = i$ és ezt akartuk bizonyítani. ∎

Lényegében elérkeztünk célunkhoz: minden rendelkezésünkre áll ahhoz, hogy igazoljuk: a hatványfüggvény diophantikus.

19. Tétel*Az n^k kétváltozós függvény diophantikus.*

Bizonyítás. Elegendő azzal az esettel foglalkoznunk, mikor n és k is legalább kettő. Állítjuk, hogy ilyen feltételek mellett $y = n^k$ akkor és csak akkor, ha vannak olyan i, p, q természetes számok, hogy

$$\begin{aligned}
&i = 1 + 2k \cdot y_n(k+1),\\
&p = y_{i \cdot n}(k+1),\\
&q = y_i(k+1),\\
&4(p - yq)^2 < q^2 \qquad\qquad \left(\text{azaz } \left|y - \frac{p}{q}\right| < \frac{1}{2}\right).
\end{aligned}$$

Az előző tétel szerint ezek mind diophantikus relációk, így ha ezt igazoljuk, készen vagyunk.

Az n és k értékek egyértelműen meghatározzák i, p és q értékét, és legfeljebb egy olyan y van, amire $\left|y - \frac{p}{q}\right| < \frac{1}{2}$. Következésképp elég megmutatni, hogy az $y = n^k$ teljesíti ezt a feltételt.

Korábban (5) alatt láttuk, hogy minden $k \geq 0$-ra

$$(2a-1)^k \leq y_a(k+1) \leq (2a)^k.$$

Ezért egyrészt

$$\frac{p}{q} \leq \frac{(2in)^k}{(2i-1)^k} = n^k\left(1 - \frac{1}{2i}\right)^{-k} \leq n^k\left(1 - \frac{k}{2i}\right)^{-1} = n^k\left(1 + \frac{k}{2i-k}\right) < n^k + \frac{kn^k}{i}.$$

Itt felhasználtuk, hogy $0 < \alpha < 1$ és $k \geq 1$ esetén $(1-\alpha)^k \geq 1 - \alpha k$, valamint hogy $i \geq 1 + k$. Másrészt

$$\frac{p}{q} \geq \frac{(2in-1)^k}{(2i)^k} = n^k\left(1 - \frac{1}{2in}\right)^k \geq n^k\left(1 - \frac{k}{2in}\right) = n^k - \frac{kn^k}{2in}.$$

Így

$$-\frac{kn^k}{i} < n^k - \frac{p}{q} \leq \frac{kn^k}{2in}.$$

Ám i definíciója alapján $i = 1 + 2k \cdot y_n(k+1) \geq 1 + 2k \cdot (2n-1)^k > 2kn^k$, tehát a bal és jobb oldalak abszolút értéke egyaránt kisebb 1/2-nél:

$$\left|n^k - \frac{p}{q}\right| < \frac{1}{2},$$

amit bizonyítani akartunk. ∎

Feladatok

1.Bizonyítsuk be, hogy egy R reláció akkor és csak akkor rekurzíve felsorolható, ha van olyan p polinom, melynek az egész helyeken felvett értékei közül a nem-negatívak éppen R elemeit adják ki. Speciálisan van olyan polinom, melynek a pozitív értékei éppen a prímek.

2.Mutassuk meg, hogy olyan eljárás sincs, mely tetszőleges egész együtthatós polinomról eldöntené, hogy van-e *egészekből* álló megoldása.

3.Bizonyítsuk be, hogy van olyan polinom, melynek akkor és csak akkor nincs egész megoldása, ha a Fermat-sejtés igaz. (Ugyanez a Rieman sejtésre.)

4.Igazoljuk, hogy minden $n \geq 4$-re van n-edfokú univerzális polinom.

5.Igazoljuk, hogy nincs olyan algoritmus, ami eldöntené, hogy egy polinomnak van-e legalább 100 egész megoldása.

6.Van-e olyan polinom, aminek nincs egészekből álló megoldása, de ezt a tényt nem tudjuk igazolni?