A diofantikus egyenletek nevüket Diophantos, 3. században élt görög matematikusról kapták, aki Aritmetika című művében először foglalkozott azzal, hogy egy egyenlet (vagy egyenletrendszer) egész megoldásait megkeresse – azaz a diofantikus egyenletekkel. Az ilyen egyenletek az aritmetika megjelenése óta komoly feladat elé állították a matematikusok népes seregét, és nemritkán az ilyen egyenletek feltörhetetlen diónak látszottak. Az ún. Fermat-féle

$$x^n + y^n = z^n \ (n \geq 3)$$

egyenletről a mai napig nem tudjuk, hogy elég nagy n-ekre van-e pozitív egészekből álló (x, y, z) megoldása. Napjainkban egy fiatal német matematikus, *Gerd Faltings* egy viszonylag új matematikai apparátussal – az algebrai görbék elméletével – lényegesnek látszó lépést tett a Fermat-féle egyenlet megoldhatóságának eldöntésére. Bebizonyította, hogy $n \geq 4$ esetén a fenti egyenletnek legfeljebb véges sok, páronként relatív prím egész számokból álló (x, y, z) megoldáshármasa van

Nyomban felmerül az a kérdés, hogy mi a helyzet az

$$x^m + y^m = z^n \quad m, n \geq 2 \text{ egészek és } (m, n) = 1, \tag{1}$$

valamint

$$x^p + y^q = z^r \quad p, q, r \geq 2 \text{ egészek és } \quad (p, q) = (p, r) = (q, r) = 1 \tag{2}$$

egyenletek esetén, hány pozitív egészekből álló megoldásuk van?

Az ezeknél általánosabb

$$\begin{gathered} x_1^{p_1} + x_2^{p_2} + \ldots + x_k^{p_k} = x_{k+1}^{p_{k+1}}, \quad k \geq 2,\, p_i \geq 2 \quad \text{egész és } (p_i, p_j) = 1 \ \text{ minden} \\ 1 \leq i < j \leq k+1 \quad \text{esetén,} \end{gathered} \tag{A}$$

illetve

$$x_1^p + x_2^p + \ldots + x_k^p = x_{k+1}^q, \quad p, q \geq 2 \quad \text{egész és} \quad (p, q) = 1 \tag{B}$$

egyenletekről fogjuk bebizonyítani, hogy mind az (A), mind a (B) típusú egyenleteknek végtelen sok természetes egészekből álló $(x_1, x_2, \ldots, x_k)$ megoldása van.

Először az (A) egyenlettel foglalkozunk. Ennek megoldásait keressük az alábbi alakban:

$$x_i = k^{\alpha_i} \quad 1 \leq i \leq k+1, \tag{$a1$}$$

ahol legyen α_i olyan egész szám, hogy

$$\alpha_i p_i = \lambda \quad 1 \leq i \leq k, \tag{$a2$}$$

valamilyen fix λ-ra. Ezekkel az (A) a következőképpen alakul:

$$k \cdot k^{\lambda} = k^{p_{k+1}\alpha_{k+1}}, \tag{$a3$}$$

ami azt jelenti, hogy

$$p_{k+1}\alpha_{k+1} - \lambda = 1. \tag{$a4$}$$

Az $(a2)$ miatt $p_i|\lambda$, és $i \neq j$ mellett $(p_i, p_j) = 1$, így $p_1 p_2 \ldots p_k|\lambda$, azaz létezik olyan q pozitív egész, amelyre $p_1 p_2 \ldots p_k q = \lambda$. Jelölje P a $p_1 p_2 p_3 \ldots p_k$ szorzatot. $(a2)$-ből

$$\alpha_i = p_1 p_2 \ldots p_{i-1} p_{i+1} \ldots p_k q = \frac{P}{p_i} q,$$

és $(a4)$-ből

$$p_{k+1}\alpha_{k+1} - p_1 p_2 \ldots p_k q = p_{k+1}\alpha_{k+1} - Pq = 1. \tag{$a5$}$$

Ismeretes, hogy ha $(a, b) = 1$, akkor az $ax - by = 1$ elsőfokú, diofantikus egyenletnek végtelen sok (x, y) egészekből álló megoldása van, és valamennyi megoldás

$$\begin{aligned} x &= x_0 + bt \\ y &= y_0 + at \end{aligned} \tag{$a6$}$$

alakban írható fel, ahol (x_0, y_0) egy tetszőleges megoldás, t pedig valamilyen egész szám. (Lásd: dr. Szendrei János: Algebra és számelmélet. 151. oldal, Tankönyvkiadó). Ha most a és b pozitívak, akkor van olyan t' pozitív egész, amely mellett minden t'-nél nem kisebb t-re az $(a6)$ szerint adódó x és y is pozitív, azaz végtelen sok pozitív egész megoldása van az $ax - by = 1$ egyenletnek.

Visszatérve $(a5)$-re, mivel $(p_i,\, p_j) = 1 (i \neq j)$, ezért $(p_{k+1}, P) = 1$ is igaz, így az $(a5)$ egyenletnek végtelen sok $(\alpha_{k+1},\, q)$ pozitív egész megoldása van, és a megoldások

$$\alpha_{k+1} = \alpha_0 + p_1 p_2 \dots p_k t = \alpha_0 + Pt,$$
$$q = q_0 + p_{k+1} t$$

alakban írhatók, ahol $t > \max\left(-\dfrac{\alpha_0}{P},\, -\dfrac{q_0}{p_{k+1}}\right)$ és egész, α_0, q_0 pedig $(a5)$-nek egy tetszőleges megoldása. Az $(a1)$–$(a5)$ egyenletekből nyert

$$x_i = k^{p_1 p_2 \dots p_{i-1} p_{i+1} \dots p_k (q_0 - p_{k+1} t)} = k^{\frac{P}{p_i}(q_0 + p_{k+1} t)} \qquad 1 \le i \le k$$

és

$$x_{k+1} = k^{p_1 p_2 \dots p_k t + \alpha_0} = k^{Pt + \alpha_0}$$

szolgáltatják az (A) egyenletnek végtelen sok pozitív egész megoldását.

Rátérve most a (B) egyenletre, ennek megoldásait

$$x_i = k^{\alpha}, \quad x_{k+1} = k^{\beta} \tag{b1}$$

alakban keressük, ahol α és β meghatározandó pozitív egészek.

$$k \cdot k^{\alpha p} = k^{\beta q}, \tag{b2}$$

ami akkor és csak akkor teljesül, ha

$$q\beta - p\alpha = 1. \tag{b3}$$

Mivel $(p,\, q) = 1$, ezért a már idézettek miatt $(b3)$-nak végtelen sok egész megoldása van, és minden megoldás

$$\beta = \beta_0 + pt, \qquad \alpha = \alpha_0 + qt \tag{b4}$$

alakú, ahol $(\alpha_0,\, \beta_0)$ egy megoldása $(b3)$-nak, t pedig tetszőleges egész. Ha most $t > \max\left(-\dfrac{\beta_0}{p},\, -\dfrac{\alpha_0}{q}\right)$, akkor $(b4)$ pozitív egész megoldást szolgáltat. $(b3)$-nak végtelen sok pozitív egész megoldása van, s így $(b1)$ miatt

$$(1 \le i \le k) \quad x_i = k^{\alpha_0 + qt}, \quad x_{k+1} = k^{\beta_0 + pt}$$

a (B) egyenletnek végtelen sok pozitív egész megoldását adja.

Könnyen látható, hogy az alábbi két egyenletnek is végtelen sok természetes szám megoldása van:

$$x_1^{p_1} + x_2^{p_2} + \dots + x_k^{p_k} = x_{k+1}^{p_{k+1}} + x_{k+2}^{p_{k+2}} + \dots + x_{k+r}^{p_{k+r}} \quad (r \neq k), \tag{C}$$
$$x_1^{p} + x_2^{p} + \dots + x_k^{p} = x_{k+1}^{q} + x_{k+2}^{q} + \dots + x_{k+r}^{q} \quad (r \neq k), \tag{D}$$

ha a kitevőkre az (A) illetve (B)-ben felírt megszorítások fennállanak. Ezeket az egyenleteket ugyanis az (A), illetve (B) típusúakra vezethetjük vissza, ha az általánosság megszorítása nélkül feltesszük, hogy $k > r$, továbbá az $s = k - r + 1$ jelöléssel

$$x_{s+1}^{p_{s+1}} = x_{k+2}^{p_{k+2}}, \dots, x_k^{p_k} = x_{k+r-1}^{p_{k+r-1}}.$$

Módszerünk sajnos alkalmatlan a Fermat-féle egyenlet tárgyalására, hiszen lényegesen kihasználtuk a kitevők relatív prím voltát.