Bizonyítások

Végtelen sok prímszám létezik

1. Bizonyítás:

(Euklidész ie. kb. 300)

Bizonyítsunk indirekt módon. Tegyük fel, hogy véges sok létezik, ezek legyenek:

$$2;3;5;\mathbf{K}\,p$$

Képezzünk egy számot úgy, hogy összeszorozzuk a prímszámokat és hozzáadunk 1-et:

$$A = 2\cdot 3\cdot 5\cdot \mathbf{K}\cdot p + 1$$

- Ez az **A** szám nagyobb a legnagyobb prímnél, hiszen legalább 30-szor nagyobb, tehát csak összetett lehet.
- Ugyanakkor ha megpróbáljuk az ismert prímekkel osztani, akkor mindig 1 maradékot kapunk; tehát nem osztható velük, azaz prím.

Ellentmondásra jutottunk, így a kezdeti feltevésünk nem helyes, azaz végtelen sok prím létezik. ■

2. Bizonyítás:

(Módosított Euklidész)

Bizonyítsunk indirekt módon. Tegyük fel, hogy véges sok létezik, ezek legyenek:

$$2;3;5;\mathbf{K}\,p$$

Képezzünk egy számot úgy, hogy összeszorozzuk a prímszámokat és elveszünk 1-et:

$$A = 2\cdot 3\cdot 5\cdot \mathbf{K}\cdot p - 1$$

- Ez az **A** szám nagyobb a legnagyobb prímnél, hiszen legalább 30-szor nagyobb, tehát csak összetett lehet.
- Ugyanakkor ha megpróbáljuk az ismert prímekkel osztani, akkor mindig az aktuális osztónál egyel kisebb maradékot kapunk; tehát nem osztható velük, azaz prím.

Ellentmondásra jutottunk, így a kezdeti feltevésünk nem helyes, azaz végtelen sok prím létezik. ■

3. Bizonyítás:

Megadunk egy számsorozatot úgy, hogy az első tagjának legalább 1 prímosztója van, a 2. tagjának legalább két (különböző) prím osztója van, a 3. tagjának legalább három (különböző) prím osztója van és így tovább.

Legyen sorozatunk a következő:

$$a_1 = 2$$

$$a_{n+1} = a_n\left(a_n + 1\right)$$

azaz

$a_1 = 2$ $a_2 = 6 = 2 \times 3$ $a_3 = 42 = 2 \times 3 \times 7$ ...

Bizonyítsunk teljes indukcióval. Az első elemekre igaz az állítás. Mivel $(a_n; a_n + 1) = 1$ ezért nincs 1-nél nagyobb közös osztójuk. Ha tehát a_n-nek n (különböző prím osztója van, akkor ezek a prímek nem szerepelhetnek a_n+1 prímfelbontásában, tehát a_n+1 minden, prímfelbontásában szereplő eleme különbözik a_n prímfelbontásban levő elemétől. Legrosszab esetben egy prím van a_n+1 felbontásában (azaz prím vagy prímnek hatványa), így a_{n+1} prímfelbontása legalább n+1 különböző prímet tartalmaz. ■

4. Bizonyítás:

(Fermat féle számok)

A bizonyítás során felhasználjuk, hogy a $F_n = 2^{2^n} + 1$ alakú számok egymáshoz relatív prímek.

Használjuk fel a következő tulajdonságot:

$\prod_{i=0}^{n} F_i = F_{n+1} - 2$, amit teljes indukcióval bizonyítunk!

$F_0 = 3, \; F_1 = 5 = F_0 + 2$

$\prod_{i=0}^{n+1} F_i = \prod_{i=0}^{n} F_i \times F_{n+1} = (F_{n+1} - 2) F_{n+1} = \left(2^{2^{n+1}} - 1\right)\left(2^{2^{n+1}} + 1\right) = \left(2^{2^{n+1}}\right)^2 - 1 =$

$= 2^{2^{n+2}} - 1 = F_{n+2} - 2$

Legyen $i < k$ és vizsgáljuk most $(F_i; F_k)$-t. Ekkor $(F_i; F_k) = \left(F_i; \prod F_j - 2\right)$, azaz a legnagyobb közös osztó osztója 2-nek, tehát csak 1 vagy 2 lehet. Mivel páratlan számokról van szó esetünkben, így a 2 nem jön szóba, tehát relatív prímek.

Ez viszont azt jelenti, hogy vagy prímszámok, vagy olyan prímek szorzata, amely prímek a többi számban nem fordulnak elő, tehát végtelen sok prímszám van. ■

5. Bizonyítás:

A bizonyítás során használni fogjuk a következő tételeket:

$$1+p+p^2+p^3+\mathbf{K}+p^n<\frac{1}{1-p}\text{, ha } 0<p<1$$

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\mathbf{K}+\frac{1}{n}+\mathbf{K} \qquad \text{® ¥}$$

Bizonyítsunk indirekt módon. Tegyük fel, hogy véges sok létezik, ezek legyenek:

$$2;3;5;\mathbf{K}\,p$$

Ekkor:

$$\left(1+\frac{1}{2}+\frac{1}{2^2}+\mathbf{K}\right)\left(1+\frac{1}{3}+\frac{1}{3^2}+\mathbf{K}\right)\left(1+\frac{1}{5}+\frac{1}{5^2}+\mathbf{K}\right)\mathbf{L}\left(1+\frac{1}{p}+\frac{1}{p^2}+\mathbf{K}\right)<$$

$$<\frac{1}{1-\frac{1}{2}}\times\frac{1}{1-\frac{1}{3}}\times\frac{1}{1-\frac{1}{5}}\times\mathbf{K}\times\frac{1}{1-\frac{1}{p}}=\frac{2}{2-1}\times\frac{3}{3-1}\times\frac{5}{5-1}\times\mathbf{K}\,\frac{p}{p-1}$$

ami egy véges érték, hiszen véges sok szám szorzatáról van szó.

Ugyanakkor:

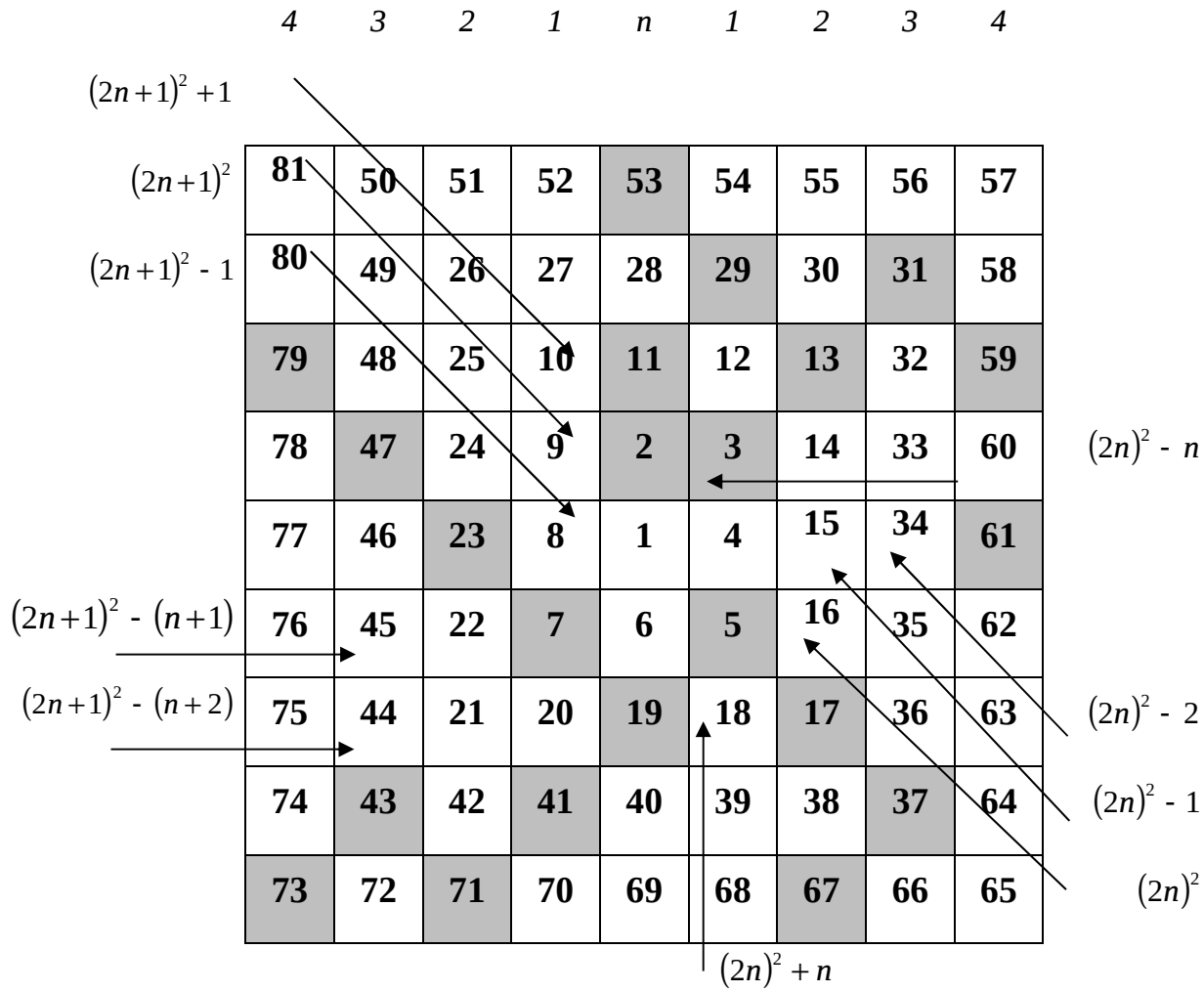
$$\left(1+\frac{1}{2}+\frac{1}{2^2}+\mathbf{K}\right)\left(1+\frac{1}{3}+\frac{1}{3^2}+\mathbf{K}\right)\left(1+\frac{1}{5}+\frac{1}{5^2}+\mathbf{K}\right)\mathbf{L}\left(1+\frac{1}{p}+\frac{1}{p^2}+\mathbf{K}\right)=$$

$$=1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\mathbf{K}+\frac{1}{n}+\mathbf{K}$$

amiről tudjuk, hogy nem véges.

Ellentmondásra jutottunk, így a kezdeti feltevésünk nem helyes, azaz végtelen sok prím létezik. ■

Prímek táblázata



$(2n+1)^2+1=2(2n^2+2n+1)$ $(2n)^2-2n=2n(2n-1)$

$(2n+1)^2=(2n+1)(2n+1)$ $(2n)^2-n=n(4n-1)$

$(2n+1)^2-1=4n(4n+1)$ $(2n)^2-2=2(2n^2-1)$ $(2n)^2+n=n(4n+1)$

$(2n+1)^2-(n+1)=n(4n+3)$ $(2n)^2-1=(2n-1)(2n+1)$

$(2n+1)^2-(n+2)=(n+1)(4n-1)$ $(2n)^2=(2n)(2n)$

Páros tökéletes számok

Kettő hatvány lehet-e?

Nézzük meg, azaz

$$\sigma(2^n) = 2 \times 2^n$$

$$2^{n+1} - 1 = 2^{n+1}$$

azaz nem lehet tökéletes szám!

Általános alak

Keressük a páros tökéletes számot $n = 2^a A$ alakban, ahol $a \geq 1$ és $A > 1$.
Ekkor

$$\sigma(n) = 2n$$

$$\sigma(2^a A) = 2 \times 2^a A$$

$$\sigma(2^a)\sigma(A) = 2^{a+1} A$$

$$(2^{a+1} - 1)\sigma(A) = 2^{a+1} A$$

$$(2^{a+1} - 1)\sigma(A) = (2^{a+1} - 1)A + A$$

$$(2^{a+1} - 1)(\sigma(A) - A) = A$$

Ez azt jelenti, hogy

$$\sigma(A) - A \mid A$$

Ekkor az **A**-nak osztói közül felsorolva 3-at:

$$1, \sigma(A) - A, A$$

Mivel még lehetnek osztói, ezért:

$$1 + \sigma(A) - A + A \leq \sigma(A)$$

$$1 + \sigma(A) \leq \sigma(A)$$

Ellentmondást kaptunk, azaz a felsorolt 3 osztó nem különböző!
A lehetőségek:
1. eset:

$A = \sigma(A) - A \Rightarrow \sigma(A) = 2A \Rightarrow A =$ páratlan tökéletes szám

és ekkor

$2^{a+1} - 1 = 1$ $a = 0$, ami nem lehet a feltételek miatt

2. eset:

$1 = \sigma(A) - A \Rightarrow \sigma(A) = A + 1 \Rightarrow A =$ prímszám

és ekkor

$2^{a+1} - 1 = A$ prímszám, ekkor
$a + 1 = p$ prím lehet csak.

Kaptuk, hogy az lehetséges alak:

$n = 2^{p-1}(2^p - 1)$ ahol $2^p - 1$=prím szám, ami Mersenne-prím. ■

Lucas-Lehmer teszt

Legyen $M_p = 2^p - 1$, ahol p prím.

valamint

$L_0 = 4$

$L_n \equiv L_{n-1}^2 - 2 \pmod{M_p}$

Ha $L_{p-2} \equiv 0 \pmod{M_p}$, akkor p prím.

$p = 5;\ M_5 = 2^5 - 1 = 31$

$L_0 = 4$

$L_1 \equiv 4^2 - 2 \equiv 14 \pmod{31}$

$L_2 \equiv 14^2 - 2 = 194 \equiv 8 \pmod{31}$

$L_3 \equiv 8^2 - 2 = 62 \equiv 0 \pmod{31}$

$p = 7;\ M_5 = 2^7 - 1 = 127$

$L_0 = 4$

$L_1 \equiv 4^2 - 2 \equiv 14 \pmod{127}$

$L_2 \equiv 14^2 - 2 = 194 \equiv 67 \pmod{127}$

$L_3 \equiv 67^2 - 2 = 4487 \equiv 42 \pmod{127}$

$L_4 \equiv 42^2 - 2 = 1762 \equiv 111 \pmod{127}$

$L_5 \equiv 111^2 - 2 = 12319 \equiv 0 \pmod{127}$

Barátságos számok

$$\left.\begin{array}{l} a = 3\times 2^n - 1 \\ b = 3\times 2^{n+1} - 1 \\ c = 3^2\times 2^{2n+1} - 1 \end{array}\right\}$$ *prímek, akkor* $\Rightarrow$ $\left\{\begin{array}{l} A = 2^{n+1}ab \\ B = 2^{n+1}c \end{array}\right.$ *barátságos számok*

Hozzuk egyszerűbb alakra a számainkat:

$$A = 2^{n+1}\left(3\times 2^n - 1\right)\left(3\times 2^{n+1} - 1\right) = 2^{n+1}\left(9\times 2^{2n+1} - 9\times 2^n + 1\right)$$

$$B = 2^{n+1}\left(9\times 2^{2n+1} - 1\right)$$

Vizsgáljuk most sz osztók összegét!

$$\sigma(A) = \sigma\left(2^{n+1}\times\left(3\times 2^n - 1\right)\left(3\times 2^{n+1} - 1\right)\right) = \sigma\left(2^{n+1}\right)\sigma\left(3\times 2^n - 1\right)\sigma\left(3\times 2^{n+1} - 1\right) =$$

$$= \left(2^{n+2} - 1\right)\times 3\times 2^n \times 3\times 2^{n+1} = 9\times 2^{2n+1}\left(2^{n+2} - 1\right)$$

$$s(A) = \sigma(A) - A = 9\times 2^{2n+1}\left(2^{n+2} - 1\right) - 2^{n+1}\left(9\times 2^{2n+1} - 9\times 2^n + 1\right) =$$

$$= 2^{n+1}\left[9\times 2^n\left(2^{n+2} - 1\right) - \left(9\times 2^{2n+1} - 9\times 2^n + 1\right)\right] =$$

$$= 2^{n+1}\left[9\times 2^{2n+2} - 9\times 2^n - 9\times 2^{2n+1} + 9\times 2^n - 1\right] =$$

$$= 2^{n+1}\left[9\times 2^{2n+2} - 9\times 2^{2n+1} - 1\right] = 2^{n+1}\left[18\times 2^{2n+1} - 9\times 2^{2n+1} - 1\right] =$$

$$= 2^{n+1}\left[9\times 2^{2n+1} - 1\right] = B$$

$$\sigma(B) = \sigma\left(2^{n+1}\left(3^2\times 2^{2n+1} - 1\right)\right) = \sigma\left(2^{n+1}\right)\sigma\left(3^2\times 2^{2n+1} - 1\right) = \left(2^{n+2} - 1\right)3^2\times 2^{2n+1}$$

$$s(B) = \sigma(B) - B = 9\times 2^{2n+1}\left(2^{n+2} - 1\right) - 2^{n+1}\left(3^2\times 2^{2n+1} - 1\right) =$$

$$= 2^{n+1}\left[9\times 2^n\left(2^{n+2} - 1\right) - \left(9\times 2^{2n+1} - 1\right)\right] =$$

$$= 2^{n+1}\left[9\times 2^{2n+2} - 9\times 2^n - 9\times 2^{2n+1} + 1\right] =$$

$$= 2^{n+1}\left[18\times 2^{2n+1} - 9\times 2^n - 9\times 2^{2n+1} + 1\right] =$$

$$= 2^{n+1}\left[9\times 2^{2n+1} - 9\times 2^n + 1\right] = A$$

Tehát ezek tényleg barátságos számok! ■

Prímértékű polinom

Használt azonosság

$$a^n - b^n = (a - b)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \mathbf{K} + a^2b^{n-2} + ab^{n-1} + b^{n-1}\right)$$

Ha $f(x_0) = p$*, akkor* $p \mid f(x_0 + p)$

Legyen $f(x) = a_n x^n + a_{n-1}x^{n-1} + \mathbf{K} + a_1 x + a_0$ és $f(x_0) = p$

$$f(x_0 + p) - f(x_0) = a_n\left[(x_0 + p)^n - x_0^n\right] + a_{n-1}\left[(x_0 + p)^{n-1} - x_0^{n-1}\right] + \mathbf{K} + a_1\left[(x_0 + p) - x_0\right]$$

Az azonosság szerint minden, kapcsos zárójelben levő kifejezés osztható **p**-vel, tehát

$p \mid f(x_0 + p) - f(x_0)$

mivel

$p \mid f(x_0) = p$, tehát $p \mid f(x_0 + p)$

Tehát nincs olyan polinom, ami minden esetre prímértéket venne fel.

Prímszám alak: a+bk

a, a+b, a+2b, a+3b, …. a+b(a-1) között egy biztosan osztható a-vel!
Ha a-vel osztjuk őket, akkor mind különböző maradékot adnak, ugyanis
TF., hogy a+bi és a+bj ugyanazt adja, akkor (a+bi)-(a+bj)=b(i-j). Itt b-vel nem lehet osztható, i-j pedig kisebb a-nál, tehát nem adhatnak egyforma maradékot.
Ekkor viszont „a” db maradékot adhatnak a-val osztva, tehát az egyik 0!