A prímszámok számáról már tudtok egyet-mást. Tudjátok azt, hogy végtelen sok prímszám van, melyek nem is túl ritkán helyezkednek el, hiszen reciprok értékeik összege tetszőleges nagyra felnőhet, ha elég sokat adunk össze belőlük, míg pl. a négyzetszámok reciprokértékének összegére ez nem igaz – ki lehet mutatni, hogy ez utóbbi sohasem lesz nagyobb 2-nél. – Az ellenkező oldalról is tudtok valamit. Az x-nél nem nagyobb prímszámok számát a $\pi(x)$-szel jelöltétek, és megmutattátok, hogy a $\pi(x) \leq \frac{x}{2}$ ha $x \geq 8$ és $\pi(x) \leq \frac{x}{3}$ ha $x \geq 33$. Ezt másképp nagyjából úgy fogalmazhatjuk, hogy ha elég messze megyünk a számsorban, akkor átlagban a számoknak legfeljebb a fele, sőt legfeljebb a harmada lehet prímszám. Ennek a fogalmazásnak jobban megfelel, ha a $\pi(x)$ helyett $\frac{\pi(x)}{x}$-et vizsgáljuk. Az előbbiek x-szel osztva így írhatók: ha $x \geq 8$ illetve $x \geq 33$, akkor $\frac{\pi(x)}{x} \leq \frac{1}{2}$, illetve $\frac{\pi(x)}{x} \leq \frac{1}{3}$. Utóbbi bebizonyítására azt használtuk fel, hogy 6 egymásutáni egész szám közül a harmadrészük, 2 relatív prím a 6-hoz, és prímszámok csak ezek lehetnek, meg még 6 prímosztói: 2 és 3. E prímosztók némi nehézséget okoztak, amit azzal lehetett kiküszöbölni, hogy kerestetek 6 egymásutáni számot (33, 34, 35, 36, 37, 38 voltak ilyenek), amelyekre már fennáll az egyenlőtlenség. Ha ezzel a módszerrel próbálnánk kimutatni, hogy $\frac{\pi(x)}{x}$ valahonnan kezdve $\frac{1}{4}$-nél,vagy $\frac{1}{5}$-nél is kisebb, akkor először is egy olyan a számot kellene keresni, hogy bármely a egymásutáni szám közül ezeknek legfeljebb $\frac{1}{4}$, illetve $\frac{1}{5}$ része legyen a-hoz relatív prím. Ilyen szám van is, mégpedig 210, illetve 30 030 a legkisebb. Ez azonban azt jelenti, hogy 210, illetve 30 030 egymásutáni számot kell keresni, melyekre mindre igaz a bizonyítandó egyenlőtlenség, ami nehézkessé teszi az eljárást, pedig általában igaz, hogy ha akármilyen kicsiny c számot adunk is meg elég nagy x-től kezdve mindig $\frac{\pi(x)}{x} < c$, vagyis $\frac{\pi(x)}{x}$ bármilyen kis számnál kisebb lesz, amint x-et elég nagynak választjuk.

Megpróbálhatjuk az előbbi gondolatot kicsit másképpen felhasználni. Eddig az x-ig terjedő egész számokat a egymásutáni számból álló csoportokra osztottuk fel és egy-egy ilyen csoportban néztük, hogy hány prímszám lehet. Választhatnánk az a-t akkorának, bogy az a-ig terjedő egész számok közt legyenek az x-ig terjedők mind; pl. választhatnánk, ha most x egész szám, a-nak magát az x-et is. Jelöljük x egymásutáni egész szám közt az x-hez relatív prímek számát $\varphi(x)$-szel, akkor $\pi(x)$ nem lehet nagyobb, mint $\varphi(x)$, hozzávéve még x különböző prímosztóinak számát, mert ezek prímszámok, azonban x-hez nem relatív prímek. Ez azonban nem mindig ad jó becslést $\pi(x)$-re, mert, ha például $x = p$ prímszám, akkor, mivel p egymás utáni szám között p-nek csak egy többszöröse fordul elő, így $\varphi(p) = p-1$, ehhez jön még x különböző prímosztóinak a száma, ami most 1, tehát egy p prímszámra nézve csak a következő magától értetődő egyenlőtlenséget kapjuk

$$\pi(p) \leq (p-1) + 1 = p$$

(az első p szám között nem lehet több prímszám, mint ahány szám van). a-nak azonban nem kell magát x-et választanunk. Ha találunk egy x-nél nagyobb számot, melyhez kevés a hozzá relatív prímek száma, akkor előnyösebb lesz azt választanunk. Első feladatunk tehát, egy számhoz relatív prím számok számát, az úgynevezett „Euler-féle $\varphi(n)$ függvényt" közelebbről megismerni.

*

Az n egymásutáni szám közül az n-hez relatív prím számok számát jelöltük így. Első kérdés, hogy ez a $\varphi(n)$ függvény nem függ-e attól is, hogy hol választjuk ezt az n egymásutáni számot? Legyen n egymás utáni szám

$$a,\ (a+1),\ \ldots (a+n-1),$$

és ugyanígy

$$(a+1),\ \ldots (a+n-1),\quad (a+n).$$

Ha bebizonyítjuk, hogy mindkét sorozatban ugyanannyi n-hez relatív prím szám van, akkor, mivel egyenkénti „eltolással" bármely egymásutáni n számig eljuthatunk, bármely egymás utáni n darab egész számra ugyanaz lesz a $\varphi(n)$ értéke is.

Tekintettel arra, bogy az $(a+1),\ \ldots (a+n-1)$ számok a két sorozatban megegyeznek, csak azt kell belátni, hogy, ha az a és $(a+n)$ számok valamelyike n-hez relatív prím, a másik is az lesz. Ennél azonban többet fogunk bizonyítani; azt, hogy a és n legnagyobb közös osztója ugyanaz, mint $(a+n)$ és n-é, vagyis $(a,\ n) = (a+n,\ n)$.

Ugyanis a-nak és n-nek minden osztója így a legnagyobb, közös osztójuk is osztója $(a+n)$-nek, másrészt $a = (a+n) - n$ felírásból következik, hogy viszont $(a+n)$ és n minden osztója, tehát legnagyobb közös osztójuk is osztója a-nak, ami azt jelenti, hogy

$$(a,\ n) = (a+n,\ n).$$

Legegyszerűbb tehát a $\varphi(n)$ függvényt úgy értelmezni, bogy az n-ig terjedő pozitív egész számok között az n-hez relatív prímek számát jelenti.

Hogyan lehet most már a $\varphi(n)$ függvényt kiszámítani? Kezdjük a legegyszerűbb esettel. Ha $n = p$ prímszám, akkor hozzá az 1, 2, $\ldots$ $(p-1)$ számok mind relatív prímek, csak maga p nem az, így $\varphi(p) = p-1$. Nézzük meg most egy prímszám hatványát. p^α-hoz csak a p-vel osztható számok nem relatív prímek, tehát p, $2p$, $\ldots$, $p^{\alpha-1}p$, s ezek száma $p^{\alpha-1}$. Így $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Amit így is írhatunk:

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1) = p^{\alpha-1}\varphi(p). \tag{1}$$

Legyen most p és q két különböző prímszám, és keressük $\varphi(p \cdot q)$ értékét. Írjuk fel 1-től $p \cdot q$-ig a számokat, a következőképpen:

$$\begin{array}{rrcrr}
1, & 2, & \ldots\ldots, & p-1, & p, \\
p+1, & p+2, & \ldots\ldots, & 2p-1, & 2p, \\
 & & \ldots\ldots & & \\
(q-2)\,p+1, & (q-2)\,p+2, & \ldots\ldots, & (q-1)\,p-1, & (q-1)\,p, \\
(q-1)\,p+1, & (q-1)\,p+2, & \ldots\ldots, & q\,p-1, & q\,p.
\end{array}$$

Az első sorban nyilvánvalóan $\varphi(p)$ számú p-hez relatív prím szám van (az utolsó kivételével mind az) – $\varphi(p)$ szám relatív prím a p-hez a többi sorban is, hiszen bármely p egymásutáni szám között $\varphi(p)$ relatív prím szám van a p-hez. Könnyen belátható, hogy ezek úgy helyezkednek el, bogy egy-egy oszlopban, vagy csupa p-hez relatív prím szám van, vagy egyik szám sem ilyen. Emlékezzünk csak vissza arra – amit fentebb bizonyítottunk –, hogy $(a,\, n) = (a+n,\, n)$. Ebből n helyett p-t téve azonnal következik állításunk, mert egy-egy oszlopban egymás alatt mindig, épp p-vel különböző számok következnek. Nézzük most, mely számok lesznek q-hoz relatív prímek. Ezt oszloponként lesz célszerű megvizsgálni. Tulajdonképpen csak azok az oszlopok érdekelnének, amelyben p-hez relatív prím számok állnak, de nézzük egyelőre mindegyiket. Az utolsó oszlopban azok lesznek relatív prímek a q-hoz, melyekben p szorzója q-hoz relatív prím, hisz p-nek nincs közös osztója q-val. Ezek a szorzók pedig az 1, 2, … $(q-1)$, q számok. Köztük $\varphi(q) = (q-1)$ számú q-hoz relatív prím szám van. Maguk a p, $2p$, …, $(q-1)p$, qp számok nagyobbak az 1., 2., …, $q-1$, q számoknál, egy szempontból mégsem különböznek tőlük lényegesen. Ha elosztjuk őket q-val, a maradék közt az első q szám mindegyike előfordul. (Persze, akkor a maradék nélküli osztás helyett q maradékot írunk: $p \cdot q = (p-1)q + q$).

Mielőtt ezt belátnánk, megjegyezzük, hogy ebből is következtethetünk arra, hogy hány q-hoz relatív prím szám van az oszlopban. Azok lesznek a q-hoz relatív prím számok, melyeknek az osztási maradéka relatív prím a q-hoz. Legyen ugyanis az $a : q$ osztás (egész) hányadosa h, maradéka m, ez azt jelenti, hogy $a = q \cdot h + m$ amiből azonnal következik állításunk.

A p, $2p$, …, $(q-1)p$, qp számokról azt mutatjuk meg, hogy nem lehet köztük kettő, mely q-val osztva ugyanazt a maradékot adja. Ha ugyanis $kp = qh_1 + m$ és $lp = qh_2 + m$ volna, egyenlő maradékkal, akkor $(k-l)p = (h_1 - h_2)q$ kellene hogy legyen. De mivel p és q relatív prímek, ez csak úgy lehetne igaz, ha $(k-l)$ többszöröse lenne q-nak. Ez azonban különböző k és l esetén lehetetlen, mert mindegyikük az 1, 2, …, $(q-1)$, q, számok közül való, így különbségük legfeljebb $q-1$ lehet, és így nem lehet osztható q-val.

A maradékok tehát mind különbözők, az 1, 2, …, $(q-1)$, q számok közül valók, és számuk q. Ez pedig csak úgy lehet, ha a maradékok között az 1, 2, …, $(q-1)$, q számok mindegyike előfordul és mindegyik csak egyszer.

Ebből a meggondolásból könnyen következtethetünk az előző oszlop q-hoz relatív prím számainak számára is. Az előző oszlopban ugyanis minden szám eggyel kisebb, mint az utolsó oszlop ugyanannyiadik sorában álló, tehát q-val osztva, eggyel kisebb lesz az osztás maradéka is. Ennek az oszlopnak a maradékai tehát a 0, 1, …, $(q-1)$ számok lesznek (persze általában nem ebben a sorrendben). A 0 maradék azt jelenti, hogy a megfelelő szám osztható q-val. Ezt az osztást így megint felírhatjuk, ha tetszik q maradékkal is és akkor ebben az oszlopban is ugyanazok a maradékok, mint az utolsó oszlopban, csak más sorrendben. A q-hoz relatív prím számok száma is ugyanannyi ebben az oszlopban is, mint az utolsóban volt, azaz $\varphi(q)$.

Ha most ismét a megelőző (végéről harmadik) oszlopra térünk át, ott megint eggyel csökkennek a számok minden sorban, és így szó szerint megismételve a gondolatmenetet beláthatjuk, hogy ebben is és mindegyik oszlopban $\varphi(q)$ a q-hoz relatív prímszámok száma.[1]

Az előzőekben láttuk, hogy $\varphi(p)$ olyan oszlop van, melyben levő számok p-hez relatív prímek. Másrészt minden oszlopban, tehát minden ilyen oszlopban is $\varphi(q)$ szám lesz relatív prim a q-hoz is, így az első $p \cdot q$ szám között $\varphi(p) \cdot \varphi(q)$ lesz a $p \cdot q$-hoz relatív prím számok száma, vagyis $\varphi(p \cdot q) = \varphi(p)\varphi(q) = (p-1)(q-1)$.

Ebben a bizonyításban nem használtuk ki azt, hogy p és q prímszámok, csupán csak azt, hogy relatív prímek. (Akkor, mikor azt mondtuk, hogy a p, $2p$, …, $(q-1)p$, qp számok közül azok és csakis azok relatív prímek q-hoz, melyekben p-nek a szorzója relatív prím a q-hoz, meg mikor abból, hogy q osztója kell legyen $(k-l)p$-nek arra következtettünk, hogy $(k-l)$-nek is osztója kell legyen.) Így általában, ha P és Q tetszőleges egymáshoz relatív prím számok (tehát általában nem prímek), akkor is mindig igaz, hogy $\varphi(P \cdot Q) = \varphi(P) \cdot \varphi(Q)$. Ezzel azonban már ki is tudjuk számítani a φ-függvény értékét egy tetszőleges a helyen, hisz a-t fel tudjuk bontani páronként relatív prím tényezők szorzatára, tudniillik különböző prímszámok hatványaira:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_{n-1}^{\alpha_{n-1}} \cdot p_n^{\alpha_n}.$$

[1] Megmutathattuk volna közvetlenül is, hasonlóan, mint az utolsó oszlopban tettük, hogy bármelyik oszlopban két különböző szám különböző maradékot ad q-val osztva. Ebből is következnék, hogy egy-egy oszlopban $\varphi(q)$ a q-hoz relatív prím számok száma.

Így lépésről lépésre alkalmazva eredményeinket kapjuk, hogy

$$\begin{aligned}\varphi(a) &= \varphi\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_{n-1}^{\alpha_{n-1}}\cdot p_n^{\alpha_n}\right) = \\ &= \varphi\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_{n-1}^{\alpha_{n-1}}\right)\varphi\left(p_n^{\alpha_n}\right) = \ldots = \\ &= \varphi\left(p_1^{\alpha_1}\right)\cdot\varphi\left(p_2^{\alpha_2}\right)\cdot\ldots\cdot\varphi\left(p_{n-1}^{\alpha_{n-1}}\right)\cdot\varphi\left(p_n^{\alpha_n}\right) = \\ &= p_1^{\alpha_1-1}(p_1-1)\cdot p_2^{\alpha_2-1}(p_2-1)\cdot\ldots\cdot p_{n-1}^{\alpha_{n-1}-1}(p_{n-1}-1)\cdot p_n^{\alpha_n-1}(p_n-1) = \\ &= p_1^{\alpha_1-1}\cdot p_2^{\alpha_2-1}\cdot\ldots\cdot p_{n-1}^{\alpha_{n-1}-1}p_n^{\alpha_n-1}(p_1-1)(p_2-1)\ldots(p_{n-1}-1)(p_n-1).\end{aligned}$$

A zárójeles tényezők rendre $\varphi(p_1)$, $\varphi(p_2)$, …, $\varphi(p_{n-1})$, $\varphi(p_n)$. Így az utolsó alakból azt is kiolvashatjuk, hogy ha $a = p^\alpha b$ és b még osztható p-vel, akkor

$$\varphi(p^\alpha b) = p^\alpha\varphi(b) \tag{2}$$

(Felhasználtuk, hogy, ha p_n különbozik p_1, …, p_{n-1} törzsszámoktól, akkor $\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\ldots p_{n-1}^{\alpha_{n-1}}, p_n^{\alpha_n}\right) = 1$ és az (1) formulát.) Mivel azonban a $\dfrac{\pi(x)}{x}$ értékéről szeretnénk valamit tudni, inkább a $\dfrac{\varphi(a)}{a}$ értéke érdekel minket, amit pedig a fenti egyenlőségből a-val való osztás után kapunk:

$$\begin{aligned}&\frac{\varphi(a)}{a} = \\ &= \frac{p_1^{\alpha_1-1}p_2^{\alpha_2-1}\ldots p_{n-1}^{\alpha_{n-1}-1}p_n^{\alpha_n-1}(p_1-1)(p_2-1)\ldots(p_{n-1}-1)(p_n-1)}{p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{n-1}^{\alpha_{n-1}}p_n^{\alpha_n}} \\ &= \frac{(p_1-1)(p_2-1)\ldots(p_{n-1}-1)(p_n-1)}{p_1p_2\ldots p_{n-1}p_n} = \\ &= \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_{n-1}}\right)\left(1-\frac{1}{p_n}\right).\end{aligned}$$

*

Most térjünk vissza a $\pi(x)$ függvényre. Azt már tudjuk, hogy $\pi(x) \le \varphi(x) + (x$ prímosztóinak száma).

Azonban – mint már említettük –, ha olyan x-et veszünk, amely prímszám, vagy akár csak kevés prímtényezője van, akkor $\varphi(x)$ értéke igen nagy lesz. – Ez látható abból is, hogy $\dfrac{\varphi(a)}{a}$ értéke csupán a prímosztóitól függ, azok hatványaitól nem. – Pl. $2310 = 2\cdot3\cdot5\cdot7\cdot11$, 2309 prímszám, és $2304 = 2^8\cdot3^2$. Nézzük most meg, mit tudunk mondani e három szám alatti prímszámok számáról.

$$\begin{aligned}\pi(2310) &\le \varphi(2310)+5 = \varphi(2)\varphi(3)\varphi(5)\varphi(7)\varphi(11)+5 = \\ &= 1\cdot2\cdot4\cdot6\cdot10+5 = 485; \\ \pi(2309) &\le \varphi(2309)+1 = 2308+1 = 2309; \\ \pi(2304) &\le \varphi(2304)+2 = \varphi(2^8)\cdot\varphi(3^2)+2 = \\ &= 2^7(2-1)\,3\,(3-1)+2 = 2^8\cdot3+2 = 770.\end{aligned}$$

A második és harmadik egyenlőtlenség helyett lényegesen jobbat kapunk felhasználva, hogy $\pi(2309) \le \pi(2310)$, valamint $\pi(2304) \le \pi(2310)$.[2]

Így:

$$\pi(2309) \le 485, \quad \text{és} \quad \pi(2304) \le 485.$$

Mi igyekszünk $\pi(x)$ számára lehetőleg jó egyenlőtlenséget, lehetőleg kis felső korlátot keresni. Ehhez célszerű olyan számot keresnünk, mely x-nél egyrészt nem sokkal nagyobb, másrészt sok prímosztója legyen, éspedig minél kisebb hatványkitevővel, azonkívül jó, ha ezek a prímszámok minél kisebbek. (Pl.: $2\cdot3\cdot67 = 402 > 5\cdot7\cdot11 = 385$, és mégis $\varphi(2\cdot3\cdot67) = 132$ és $\varphi(5\cdot7\cdot11) = 240$ – a 2 és 3 miatt.)

Vegyük e célból az első n egymásutáni prímszám szorzatát, jelöljük P_n-nel $P_n = p_1p_2\ldots p_n$. Biztos, hogy van egy olyan n, melyre $P_n < x \le P_{n+1}$ egyenlőtlenség fennáll. Vegyük most a P_n, $2P_n$, … számokat. Lesz köztük két szomszédos, amelyek közé esik x, megengededve, hogy pl. a nagyobbikkal esetleg egybe is eshetik. Legyen ez $k\cdot P_n$ és $(k+1)P_n$. Ekkor $k\,P_n < x \le (k+1)P_n \le P_{n+1} = p_{n+1}P_n$ és így $k < p_{n+1}$, $k+1 \le p_{n+1}$. Mivel $x \le (k+1)P_n$

$$\pi(x) \le \pi\big([k+1]P_n\big)$$

[2] Ez utóbbiról tudjuk, hogy határozottan kisebb, hiszen közöttük van egy prímszám, ugyanis 2309

$(k+1)P_n$-ben legfeljebb $n+1$ különböző prímtényező szerepel, ugyanis, ha $k+1=p_{n+1}$, akkor a p_1, p_2, …, p_n, p_{n+1} tényezők, ha pedig $k+1<p_{n+1}$, akkor $k+1$ is csak a p_1, p_2, …, p_n tényezőket tartalmazhatja. Így

$$\pi\big([k+1]P_n\big)\le\varphi\big([k+1]P_n\big)+(n+1)$$

Amennyiben $k+1=p_{n+1}$, akkor $(p_{n+1},P_n)=1$ folytán $\varphi\big([k+1]P_n\big)=(p_{n+1}-1)\varphi(P_n)<(k+1)\varphi(P_n)<(k+1)\varphi(P_n)$. Ha $k+1<p_{n+1}$ akkor $k+1$ tényezőia P_n-ben már szerepelnek, így a (2) alapján $(k+1)$-et „kiemelhetjük”, vagyis $\varphi\big([k+1]P_n\big)=(k+1)\varphi(P_n)$. Így mindkét esetben

$$\varphi\big([k+1]P_n\big)\le(k+1)\varphi(P_n).$$

Ezt felhasználva azt nyertük, hogy $\pi(x)\le(k+1)\varphi(P_n)+n+1$. Kérdés most, hogyan kaphatunk felső korlátot $\dfrac{\pi(x)}{x}$ számára? A számláló helyett sikerült nála nagyobb, jobban kezelhető kifejezést találnunk. Jó volna a nevezőt is P_n egy többszörösével helyettesíteni. Ha biztosak akarunk lenni benne, hogy továbbra is $\pi(x)$-nél nagyobb értéket kapunk, akkor ezt úgy kell megtennünk, hogy a jobboldal ne csökkenjen közben. Ha a nevezőt csökkentjük, akkor fog növekedni a tört értéke. Tegyük hát az x helyébe a nála kisebb $k\cdot P_n$-et, így

$$\frac{\pi(x)}{x}<\frac{(k+1)\varphi(P_n)+n+1}{kP_n}=\frac{(k+1)\varphi(P_n)}{kP_n}+\frac{n+1}{kP_n}=$$
$$=\frac{k+1}{k}\frac{\varphi(P_n)}{P_n}+\frac{n+1}{kP_n}.$$

Erről akarjuk megmutatni, hogy tetszőlegesen kicsiny lesz, amint n elég nagy (s így még inkább igaz lesz ez $\dfrac{\pi(x)}{x}$-re). Ez várhatóan azon fog múlni, hogy ugyanez igaz $\dfrac{\varphi(P_n)}{P_n}$-re. Hagyjuk ezt a kifejezést utoljára és vizsgáljuk előbb a könnyebben letárgyalhatókat. Nézzük először a második tagot. Itt a nevezőben P_n utolsó két tényezőjének szorzata is már lényegesen nagyobb a számlálónál. Pontosan ez így követhető számítással. Mivel az első prímszám, $p_1=2$ nyilván minden prímszámra $p_n\ge n+1$, sőt $p_3=5$ folytán, ha $n>5$, akkor az egyenlőség nem állhat fenn, vagyis $p_n>n+1$ és $p_{n-1}\ge n$. Ez esetben

$$\frac{n+1}{k\cdot p_1\dots p_{n-1}p_n}<\frac{n+1}{n(n+1)}<\frac{1}{n}.$$

A másik tört első tényezőjére $k+1\le 2k$, vagyis $\dfrac{k+1}{k}\le 2$. Így maradt a tulajdonképpeni feladat $\dfrac{\varphi(P_n)}{P_n}$ megbecslése. Tudjuk, hogy $P_n=p_1\cdot p_2\cdot\ldots\cdot p_n$, s így

$$\frac{\varphi(P_n)}{P_n}=\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_n}\right).$$

Azt kellene bizonyítanunk, hogy ez a szorzat is tetszőlegesen kicsivé tehető, ha n-et elég nagyra választjuk. Könnyebb azonban olyan állításokat bizonyítani, hogy valamilyen kifejezés „nagyon naggyá válhat”, így ennek megfelelően átalakítjuk feladatunkat. Az, hogy bármekkora pozitív szám is c (bármilyen kicsi is lehet tehát), egy elég nagy n_0-tól kezdve minden n-re

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_n}\right)<c$$

ugyanannyit jelent, mint az, hogy az n_0-nál nagyobb n-ekre

$$\frac{1}{\left(1-\dfrac{1}{p_1}\right)\left(1-\dfrac{1}{p_2}\right)\dots\left(1-\dfrac{1}{p_n}\right)}>\frac{1}{c},$$

és itt $\dfrac{1}{c}$ megint bármilyen pozitív szám, tehát bármilyen nagy is lehet. (Persze megfelelően nagyra kell akkor az n-et is választani.) De

$$\frac{1}{\left(1-\dfrac{1}{p_1}\right)\left(1-\dfrac{1}{p_2}\right)\dots\left(1-\dfrac{1}{p_n}\right)}=\frac{1}{\left(1-\dfrac{1}{p_1}\right)}\cdot\frac{1}{\left(1-\dfrac{1}{p_2}\right)}\dots\frac{1}{\left(1-\dfrac{1}{p_n}\right)}$$

Ha az egyes tényezők számlálójában még egy $\left(\frac{1}{p}\right)^{\alpha+1}$ alakú kivonandó szerepelne, akkor ráismernénk a mértani sor összegére, s így könnyen meggyőződhetünk arról, hogy

$$\frac{1}{1-\frac{1}{p_i}} > \frac{1-\left(\frac{1}{p_i}\right)^{\alpha_i+1}}{1-\frac{1}{p_i}} = 1+\frac{1}{p_i}+\cdot\cdot+\frac{1}{p_i^{\alpha_i}}.$$

(itt p_i jelentheti a p_1, p_2, …, p_n számok bármelyikét, α_1, α_2, …, α_n pedig tetszőleges pozitív egész számokat. Ezt alkalmazva sorra p_1, p_2, …, p_n-re

$$\frac{1}{\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_n}\right)} > \left(1+\frac{1}{p_1}+\frac{1}{p_1^2}+\dots+\frac{1}{p_1^{\alpha_1}}\right)\left(1+\frac{1}{p_2}+\dots+\frac{1}{p_2^{\alpha_2}}\right)\dots\left(1+\frac{1}{p_n}+\dots+\frac{1}{p_n^{\alpha_n}}\right).$$

Ha minden tagot minden taggal összeszorzunk, ilyen tagokat kapunk:

$$\frac{1}{p_1^{\beta_1}p_2^{\beta_2}\dots p_n^{\beta_n}},$$

ahol a β-k a megfelelő α-knál nem nagyobb pozitív számok, vagy lehet bármelyikük 0 is (ha a megfelelő tényezőből az 1-gyet választottuk ki szorzóul). Mivel bármely p_n-nél nem nagyobb szám prímtényezői a p_1, p_2, …, p_n között vannak, bármelyiket felírhatjuk ilyen alakban, így a beszorzásnál ezek mindegyikének reciprokát megkapjuk, ha az α-kat elég nagynak választjuk. Ezekről eddig semmit sem kötöttünk ki, tehát még szabadon megválaszthatjuk őket. Legyen pl. minden α akkora, hogy a megfelelő $p_i^{\alpha_i} > p_n$ legyen. De kapunk p_n-nél nagyobb számok reciprokait is, így

$$\frac{1}{\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_n}\right)} > 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\dots+\frac{1}{p_n-1}+\frac{1}{p_n}.$$

Nézzük ennek a sornak az elejét

$$1=1,\quad \frac{1}{2}=\frac{1}{2},\quad \frac{1}{3}+\frac{1}{4}>\frac{1}{4}+\frac{1}{4}=\frac{1}{2},\quad \frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}>\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}=\frac{4}{8}=\frac{1}{2}$$

. Tovább is hasonlóan haladhattunk: 2 egyik hatványától a következőig a részletösszeg nagyobb, mint $\frac{1}{2}$:

$$\frac{1}{2^{l-1}+1}+\frac{1}{2^{l-1}+2}+\dots+\frac{1}{2^l}>\frac{1}{2^l}+\dots+\frac{1}{2^l}=$$
$$=2^{l-1}\frac{1}{2^l}=\frac{1}{2},$$

mert a tagok száma 2^{l-1}. Ha most a sorban 1-től 2^l-ig megyünk, az első 1-es után l számú $\frac{1}{2}$-nél nagyobb ilyen összeget jelölhetünk ki s így

$$1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\dots+\left(\frac{1}{2^{l-1}+1}+\dots+\frac{1}{2^l}\right)>1+\frac{l}{2}.$$

Válasszuk most l-et úgy, hogy p_n 2-nek az l-edik és $(l+1)$-edik hatványa közé essen:

$$2^l < p_n < 2^{l+1}. \tag{3}$$

Tehát most már azt tudjuk, hogy

$$\frac{\pi(x)}{x} < 2\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_n}\right)+\frac{1}{n} < 2\frac{1}{1+\frac{l}{2}}+\frac{1}{n}=\frac{4}{l+2}+\frac{1}{n},$$

ahol l értékét a (3) egyenlőtlenség határozza meg.

$\frac{1}{n}$ tetszőlegesen kicsi, ha n nagyon nagy szám. Másrészt, ha p_n nagy, akkor l is nagy, mert (3) jobboldali egyenlőtlenségét 2-vel osztva kapjuk, hogy $2^l > \frac{p_n}{2}$; így $\frac{4}{l+2}$ szintén igen kicsi. Például, ha azt akarjuk, hogy $\frac{\pi(x)}{x}$ $\frac{1}{100}$-nál

kisebb legyen, ezt elérhetjük, ha sikerül n-et úgy választani, hogy $\frac{4}{l+2}$ és $\frac{1}{n}$ mindegyike $\frac{1}{200}$-nál kisebb legyen, vagyis $\frac{1}{n} < \frac{1}{200}$, amiből $n > 200$; továbbá $\frac{4}{l+2} < \frac{1}{200}$ kell, hogy legyen, amiből

$$\frac{l+2}{4} > 200; \quad l+2 > 800 \quad l > 798,$$

ami egész biztosan teljesül, ha n-et nemcsak 200-nál választjuk nagyobbra, hanem úgy választjuk, hogy $\frac{p_n}{2} > 2^{798}$, vagyis $p_n > 2^{799}$ legyen. Hasonlóan járhatunk el, ha $\frac{1}{100}$ helyébe bármekkora pozitív c számot teszünk. Mindig találhatunk olyan alsó korlátot x értékére, amelytől kezdve $\frac{\pi(x)}{x} < c$ lesz. A most bizonyított tényt szokás a matematika nyelvén úgy mondani, hogy $\frac{\pi(x)}{x}$ 0-hoz tart, ha x minden határon túl növekszik.[3]

Feladatok:

255. Mutassátok meg, hogy az első n pozitív szám négyzetének reciprokát összeadva 2-nél kevesebbet kapunk, bármekkora szám is n.

256. Küldjétek be a pontos bizonyítását annak, hogy ha P és Q relatív prím számok, akkor $\varphi(P \cdot Q) = \varphi(P) \cdot \varphi(Q)$.

[3] A tétel itt közölt bizonyítása Eulertól származik, a szerző azonban ezt nem ismerve, önállóan talált rá. *(Szerk.)*