

Írjuk az 1-től ab -ig terjedő számokat a következő táblázatba:

1,	2,	.	.	.,	a ,
$a + 1$,	$a + 2$,	.	.	.,	$2a$,
$2a + 1$,	$2a + 2$,	.	.	.,	$3a$,
.	.	.	.	.	.
.	.	.	.	.	.
$(b - 1)a + 1$,	$(b - 1)a + 2$,	.	.	.,	ba .

Nézzük, hogyan helyezkednek el az a -hoz relatív prímszámok. Tekintsük a k -adik oszlopot: $k, a + k, 2a + k, \dots, (b - 1)a + k$.

Ezek nyilván mind relatív prímek, vagy mind nem relatív prímek a -hoz, attól függően, hogy k relatív prím-e a -hoz, vagy nem. Látjuk tehát, hogy az a -hoz relatív prímszámok $\varphi(a)$ számú oszlopban helyezkednek el.

Most vizsgáljuk a b -hez relatív prímszámok elhelyezkedését. Mint a cikkben beláttuk, egy szám akkor és csak akkor relatív prím b -hez, ha b -vel osztva, b -hez relatív prím maradékot ad. Másrészt könnyen beláthatjuk, hogy ugyanabban az oszlopban álló két szám b -vel osztva nem adhatja ugyanazt a maradékot.

Ugyanis, ha

$$\begin{aligned} k + n_1 a &= q_1 b + r \\ k + n_2 a &= q_2 b + r \quad \text{volna,} \end{aligned}$$

akkor $(n_1 - n_2)a = (q_1 - q_2)b$ vagyis $(n_1 - n_2)a$ osztható volna b -vel, de mivel a és b relatív prímek, ebből következne, hogy $(n_1 - n_2)$ osztható b -vel. Ez azonban lehetetlen, mert n_1 és n_2 b -nél kisebb pozitív számok s így különbségük is b -nél kisebb.

Tehát az egy oszlopban álló b számú szám b -vel osztva különböző maradékokat ad, s így a maradékok az összes számok 1-től b -ig. Mivel ezek között $\varphi(b)$ darab b -hez relatív prímszám van, az előbbieket szerint minden oszlopban $\varphi(b)$ számú b -hez relatív prímszám van; a $\varphi(a)$ számú a -hoz relatív prímszámokat tartalmazó oszlopban tehát összesen $\varphi(a)\varphi(b)$ számú ab -hez relatív prímszám van. Ezzel a tételt bebizonyítottuk.