ARALARINDA ASAL SAYILARIN EN KÜÇÜK ORTAK KATI

Önerme: $a, b \in \mathbb{Z}^+$ ve $(a, b) = 1$ ise $[a, b] = ab$ olur.
İspat: $[a, b] = \min\{c \in \mathbb{Z}^+ : a \mid c \text{ ve } b \mid c\}$ olduğundan ab bu kümeye ait olduğundan $[a, b] \leq ab$ olur. Bölme Algoritmasından

$$ab = [a, b]q + r, \quad 0 \leq r < [a, b]$$

olacak şekilde $q, r \in \mathbb{Z}$ sayıları vardır. $r > 0$ olsaydı, bu eşitlikten, $r \in \{c \in \mathbb{Z}^+ : a \mid c \text{ ve } b \mid c\}$ olurdu, bu ise $[a, b] = \min\{c \in \mathbb{Z}^+ : a \mid c \text{ ve } b \mid c\}$ olması ile çelişir. Öyleyse $r = 0$ olmalı, dolayısıyla (bir $q \in \mathbb{Z}$ için)

$$ab = [a, b]q$$

olur. $a, b, [a, b] \in \mathbb{Z}^+$ olduğundan $q > 0$ olacaktır. $q = 1$ olduğunu göstermek yeterlidir. $q > 1$ olduğunu varsayalım. O zaman bir p asal sayısı için $p \mid q$ olur. $p \mid ab$ olduğundan $p \mid a$ veya $p \mid b$ den biri doğru (ve $(a, b) = 1$ olduğundan diğeri yanlış) olur. $p \mid a$ durumunu ele alalım. o zaman $p \mid [a, b]$ olacaktır. $a = pa_1$, $[a, b] = ps_1$ olsun. $ab = q[a, b]$ eşitliğinde p ler kısaltılarak $a_1 b = qs_1$ bulunur. Yine $p \mid a_1 b$ ve $p \nmid b$ olduğundan $p \mid a_1$ ve bunun sonucunda $p^2 \mid a$ bulunur. Dolayısıyla $p^2 \mid [a, b]$ elde edilir. p^2 ler kısaltılıp aynı işlem tekrarlanırsa $p^3 \mid a$, $p^4 \mid a, \cdots$ şeklinde devam edilebilir. Dolayısıyla her $n \in \mathbb{Z}^+$ için $p^n \mid a$ sonucuna varılır. Fakat yeteri kadar büyük bir n (* örneğin $n = a$) için $p^n > a$ olacağından bu imkansızdır. $p \mid b$ durumu da aynı nedenle çelişkiye yol açar. Öyleyse $q > 1$ olamaz, $q = 1$ yani $[a, b] = ab$ doğru olmak zorundadır.

(*: Her $n \in \mathbb{Z}^+$ için $2^n > n$ olduğu Tümevarımla kolayca gösterilir. Bu nedenle $p^a \geq 2^a > a$ olur)