
Σε ένα μέρος της διάλεξης μπερδεψα τα «<» και τα «≤», εδώ είναι αυτό το μέρος διορθωμένο.

Γιατί τό το κόσκινο του Ερατοσθένη δουλεύει; Επειδή, αν το $m < p^2$ δεν είναι πρώτος, έχει γνήσιους διαιρέτες a, b με $m = ab$.

Ερώτηση Γίνεται $a \geq p$ και $b \geq p$;

Απάντηση όχι: τότε $m = ab \geq p \cdot p = p^2$ άτοπο.

Έστω λοιπόν (ΔΒΓ) $a < p$. Σύμφωνα με το Λήμμα 3, το a έχει κάποιο πρώτο διαιρέτη, έστω τον q . Όμως $q|a$ άρα $q \leq a$ άρα $q < p$ άρα το q είναι κάποιο από τους p_1, \dots, p_n . Επίσης $q|a|m$ άρα $q|m$.

Περίληψη Αν ο $m < p^2$ δεν είναι πρώτος τότε έχει διαιρέτη κάποιο από τους p_1, \dots, p_n , όπως ακριβώς προβλέπει ο Ερατοσθένης.