8. Αν p πρώτος φυσικός αριθμός, να αποδειχτεί ότι: (p-1)!≡-1modp (Θεώρημα Wilson)

απόδειξη

Αν p=2 ή p=3 η πρόταση είναι προφανής. Έστω p>3.
Θεωρούμε την ισοδυναμία αχ≡1modp. (1) με α∈ A={1,2,3,…,p-1}. Επειδή (α,p)=1 η (1) έχει πάντοτε λύση. Ποιο συγκεκριμένα υπάρχει πάντοτε μοναδικός αριθμός α΄∈ A τέτοιος ώστε αα΄≡1modp. Ισχύει α=α΄ αν και μόνο αν α=1 ή α=p-1. Πράγματι, α^2≡1modp ⇔ α^2-1≡0modp ⇔ p/(α-1)(α+1) ⇔ p/α-1 ή p/α+1. Αν p/α-1 τότε αφού α-1<p θα πρέπει α=1. Αν p/α+1 θα πρέπει α=p-1. Αν τώρα εξαιρέσουμε τους αριθμούς 1 και p-1 από το σύνολο A, τα υπόλοιπα στοιχεία του μπορούν να ομαδοποιηθούν σε (p-1)/3 ζευγάρια στοιχείων που είναι αντίστροφα μεταξύ τους modp. Θα έχουμε επομένως

$$2\cdot 3\cdot 4\cdot\ldots\cdot(p-1) \equiv 1 \text{ modp} \Leftrightarrow$$

$$(p-2)! \equiv 1 \text{ modp} \Leftrightarrow$$

$$(p-1)! \equiv (p-1) \text{ modp} \equiv -1 \text{ modp}.$$

παρατηρήσεις:

1. Ισχύει και το αντίστροφο του θεωρήματος Wilson. Πράγματι αν ισχύει (p-1)!≡-1modp τότε ο p πρέπει να είναι πρώτος γιατί διαφορετικά θα υπήρχε ένας πρώτος διαιρέτης του δ με δ<p. Αφού λοιπόν δ≤p-1 θα ισχύει δ/(p-1)! και συνεπώς δ/-1 άτοπο.
2. Αν α δεν διαιρεί τον (α-1)!+1 τότε ο α είναι σύνθετος.
3. Κάποιες διαφορετικές αποδείξεις του θεωρήματος μπορείτε να δείτε στον παρακάτω σύνδεσμο: http://www.math.wfu.edu/publications/Student/Caroline%20LaRoche%20Turnage%20-%20Thesis.pdf