9. (Μικρό θεώρημα του Fermat) Αν p πρώτος αριθμός και α ακέραιος πρώτος προς τον p, τότε $\alpha^{p-1}\equiv 1$ modp.

απόδειξη

Οι ακέραιοι 1,2,3,…,p-1 αποτελούν ένα πλήρες σύστημα των πρώτων κλάσεων υπολοίπων modp. Αφού (α,p)=1 το ίδιο θα συμβαίνει και με τους ακεραίους 1·α, 2·α, 3·α, …, (p-1)·α.

Πολλαπλασιάζοντας όλους τους αριθμούς των δυο παραπάνω συστημάτων υπολοίπων θα πρέπει:

1·α·2·α·…·(p-1)·α=1·2·3·…·(p-1)· $\alpha^{p-1}\equiv 1$ ·2·3·…·(p-1)modp. Όμως είναι (p, 1·2·3·…·(p-1))=1 επομένως απλοποιώντας τους κοινούς παράγοντες προκύπτει $\alpha^{p-1}\equiv 1$ modp.

Παρατήρηση: Κάποιες διαφορετικές αποδείξεις του θεωρήματος μπορείτε να δείτε στη διεύθυνση: http://www.math.wfu.edu/publications/Student/Caroline%20LaRoche%20Turnage%20-%20Thesis.pdf