$$(\alpha+1)^p \equiv (\alpha^p+1) \equiv (\alpha+1) mod p.$$

Λίγο αργότερα ο Euler παρουσίασε και τη γενίκευση

Θεώρημα Euler

Έστω $\varphi(n)$ ο αριθμός των θετικών διαιρετών που δεν ξεπερνάνε το n και είναι σχετικά πρώτοι προς αυτό, m ένας θετικός ακέραιος και α ένας άλλος έτσι ώστε $(\alpha, m) = 1$ τότε ο $\alpha^{\varphi(m)} - 1$ διαιρείται από το $m$ ή $\alpha^{\varphi(m)} \equiv 1 mod m.$

Προφανώς αν ο $m$ είναι πρώτος τότε ισχύει $\varphi(m) = m - 1$ και προκύπτει το 'μικρό' Θεώρημα του Fermat.

Το 'μικρό' Θεώρημα του Fermat είναι μεταξύ άλλων ένα κριτήριο για το αν ένας αριθμός είναι σύνθετος. Για παράδειγμα ο 63 δεν είναι πρώτος αφού

$$2^{63} = 2^{60} \cdot 2^3 = (2^6)^{10} \cdot 2^3 = 64^{10} 2^3 \equiv 2^3 \equiv 8 mod 63 \text{ και όχι } 2 mod 63$$

Θα ήταν ίσως ακόμα πιο χρήσιμο αν μπορούσαμε να δείξουμε με τη βοήθειά του, ότι ένας αριθμός είναι πρώτος. Οι Αρχαίοι Κινέζοι ήξεραν ότι αν ο $p$ είναι πρώτος τότε διαιρεί τον $2^p - 2$. Πίστευαν όμως ότι αν ο $2^\nu - 2$ διαιρείται από το $\nu$ τότε αυτός είναι πρώτος. Δυστυχώς, το αντίστροφο του Θεωρήματος δεν ισχύει όπως δείχνει το παρακάτω παράδειγμα. Οι Κινέζοι έπρεπε να φτάσουν στον $\nu = 341$ για να διαπιστώσουν ότι έκαναν λάθος.

Έστω $\nu = 341 = 11 \cdot 31$. Από το 'μικρό' Θεώρημα του Fermat έχουμε ότι $2^{10} \equiv 1 mod 11$ έτσι $2^{340} = (2^{10})^{34} \equiv 1 mod 11$. Επίσης $2^{340} = (2^5)^{68} = 32^{68} \equiv 1\ mod 31$. Κι έτσι θα έχουμε ότι $2^{340} \equiv 1 mod 341$ και πολλαπλασιάζοντας με 2 έχουμε $2^{341} \equiv 2 mod 341$ αν και ο 341 δεν είναι πρώτος.

Υπάρχουν, δηλαδή, φυσικοί αριθμοί που ικανοποιούν τη συνθήκη του Θεωρήματος για κάποιο $\alpha$ αλλά δεν είναι πρώτοι. Γενικά αν για έναν σύνθετο αριθμό ισχύει $b^{n-1} \equiv 1\ mod\ n$ για κάποιον αριθμό $b$ που είναι πρώτος προς τον $n$, τότε αυτός λέγεται ψευδοπρώτος ως προς τη βάση $b$. Συγκεκριμένα ο 341 του παραδείγματος είναι ψευδοπρώτος ως προς τη βάση 2. Το ότι είναι ψευδοπρώτος ως προς τη βάση 2 βέβαια, δε σημαίνει ότι θα ισχύει το ίδιο και για άλλες βάσεις. Μήπως αν για έναν αριθμό n βρίσκαμε μία βάση $b$ για την οποία δε θα ίσχυε το κριτήριο $b^{n-1} \equiv 1\ mod\ n$ θα σήμαινε ότι ο αριθμός $n$ είναι πρώτος; Αν η προηγούμενη πρόταση ήταν αληθής θα είχαμε ένα πολύ