απλό και γρήγορο κριτήριο για να ελέγξουμε αν ένας αριθμός είναι πρώτος. Δυστυχώς υπάρχουν σύνθετοι αριθμοί n που ικανοποιούν το παραπάνω κριτήριο για οποιαδήποτε βάση b, όπου b σχετικά πρώτος προς τον n. Αυτοί οι αριθμοί λέγονται αριθμοί Carmichael. Ο μικρότερος από αυτούς είναι ο 561. Πράγματι $561 = 3 \cdot 11 \cdot 17$. Αν $(b, 561) = 1$ τότε $(b, 3) = (b, 11) = (b, 17) = 1$. Από το 'μικρό' Θεώρημα του Fermat έχουμε $b^2 \equiv 1 mod\ 3$, $b^{10} \equiv 1 mod\ 11$, $b^{16} \equiv 1 mod\ 17$. Επομένως, $b^{560} = (b^2)^{280} \equiv 1 mod\ 3$, $b^{560} = (b^{10})^{56} \equiv 1\ mod\ 11$, $b^{560} = (b^{16})^{35} \equiv 1 mod\ 17$. Άρα $b^{560} \equiv 1\ mod\ 561$ για κάθε βάση b με $(b, 561) = 1$. Ο αριθμός 1729, ο μικρότερος που μπορεί να γραφτεί σαν άθροισμα δύο κύβων με δύο διαφορετικούς τρόπους $(1729 = 10^3 + 9^3 = 1^3 + 12^3)$, είναι αριθμός Carmichael. Οι αριθμοί αυτοί είναι πολύ σπάνιοι. Μέχρι το $1.000.000.000$ υπάρχουν μόνο 646. Παρόλα αυτά αποδείχτηκε, μόλις το 1992, ότι οι αριθμοί Carmichael είναι άπειροι.

Με τη βοήθεια του μικρού θεωρήματος του Fermat αποδεικνύεται μία πολύ σπουδαία πρόταση.

Πρόταση

Ο $2^p - 1$ όπου ο p είναι πρώτος με $p \neq 2$ διαιρείται μόνο από τους αριθμούς της μορφής $2kp + 1$ για κάποιον ακέραιο k.

Απόδειξη

Αρκεί να δείξουμε ότι οι πρώτοι διαιρέτες του $2^p - 1$ είναι της μορφής $2kp + 1$. Έστω q ένας τέτοιος. Ισχυρισμός: ο p διαιρεί τον $q - 1$. Πράγματι, αν ο p δεν διαιρεί τον $q - 1$ τότε αφού ο p είναι πρώτος θα είναι πρώτοι μεταξύ τους άρα θα υπάρχουν m, n τέτοιοι ώστε $mp + n(q - 1) = 1$. Τότε ή ο m ή ο n είναι αρνητικός, έστω ο m, άρα ο $-m$ είναι θετικός. Από την υπόθεση έχουμε ότι $2^p \equiv 1 mod q$ άρα $2^{-mp} \equiv 1 mod q$. Από το 'μικρό' Θεώρημα του Fermat προκύπτει ότι $2^{q-1} \equiv 1 mod q$ και επομένως $[2^{q-1}]^n \equiv 1 mod q$. Τελικά, $2 = 2^1 = 2^{mp+n(q-1)} \equiv 2^{n(q-1)} mod q \equiv 1 mod q$ που είναι άτοπο. Άρα ο p διαιρεί τον $q - 1$.Επίσης, ο q είναι περιττός αφού διαιρεί τον $2^p - 1$, άρα ο $q - 1$ είναι άρτιος κι έτσι ο 2 είναι διαιρέτης του $q - 1$. Τελικά ο $2p$ είναι διαιρέτης του $q - 1$. Δηλαδή $q - 1 = 2pk$ ή $q = 2kp + 1$ για κάποιον ακέραιο k.