

Minutestek

I. Legyenek a, b, c és m egészek, ahol $b > 1$ és $m > 0$, ekkor

I. a^b maradékai mod m

II. az a és b legnagyobb közös osztója

III. (ptl. b és $(a, b) = 1$ esetén) az $\left(\frac{a}{b}\right)$ Jacobi nimboldum

IV. az $ax + by = c$ lin. diof. egyenlet megoldásai és

V. az $ax \equiv c \pmod{b}$ kongruencia megoldásai

kiszámíthatók legfeljebb 5 $\log_2 b$ lépésben, ahol egy lépés azt
egy m -nő összeadást, kivonást, szorzást és maradékos osztást
jelentik.

I. Legyen $n > 2$. Ha $2^{n-1} \not\equiv 1 \pmod{n}$, akkor n biztosan összetett.

Ha $2^{n-1} \equiv 1 \pmod{n}$ akkor n "lehetőleg biztosan" prím.

D: Ha egy n összetett számra $a^{n-1} \equiv 1 \pmod{n}$ teljesül, akkor az n -et
a **alapi alprímek** nevezzük

Ha n összetett számra a fenti kongruencia minden $(a, n) = 1$
esetén teljesül, akkor az **n univerzális alprím** vagy **Carmichael**
szám.