Algarvu kontrollimise testid.

Miller-Rabin'i test

Olgu m=9

Arvutame sobiv $r=\log_2(9)\approx 3$

Kontrollime kas on algarv

0) Esitada $9-1=2^s t$ $8=2^3*1$
1) **Tsükkel A.** Kordame r korda, ehk 3 korda
    a. Valida juhuarv a vahemikus [2, m-2], olgu a=7
    b. $x:=7^t \bmod m = t^1 \bmod 9=7$
    c. $7\neq 1$ ja samuti $7\neq 9-1$
        i. **Tsükkel B.** Kordame s-1 korda, ehk 2 korda
            1. $x:=x^2 \bmod m=7^2 \bmod 9=4$
            2. $4\neq 1$
            3. $4\neq 9-1$
        ii. Väljastada „mitte algarv"
        iii. Kordame veel, kuna pidi kordama 2 korda
            1. $x:=x^2 \bmod m=4^2 \bmod 9=7$
            2. $7\neq 1$
            3. $7\neq 9-1$
        iv. Väljastada „mitte algarv"

Olgu m=11

$r=\log_2(11)\approx 4$

0) $11-1=10=2^1*5$, ehk t=5, s=1
1) **Tsükkel A.** Korrata 4 korda
    a. Juhuarv a=6
    b. $x:=6^5 \bmod 11=10$
    c. $x\neq 1$, aga x=11-1, ehk minna järgmisele A ringile
    d. Juhuarv a=5
    e. $x:=5^5 \bmod 11=1$
    f. x=1, ehk minna järgmisele A ringile
    g. Juhuarv a=7
    h. $x:=7^5 \bmod 11=10$,
    i. x=11-1, ehk minna järgmisele A ringile
    j. Juhuarv a=8
    k. $x:=8^5 \bmod 11=10$

l. x=11-1, ehk minna järgmisele A ringile
m. A ringid on lõppenud

2) Väljastada „algarv“