9.39) 223 Solovay-Strassen

Alegem martorul 2

$2^{111} = 2\cdot 4^{55} = 8\cdot 16^{27} \equiv 128\cdot 33^{13} \equiv (-13)\cdot(-26)^{6} \equiv (-13)\cdot 7^{3} \equiv (-13)\cdot 120 \equiv 1 \pmod{223}$

$\left(\frac{2}{223}\right) = (-1)^{\frac{223^2-1}{8}} = 1 \equiv 2^{\frac{223-1}{2}} \pmod{223} \Rightarrow$ 223 trece testul pt. martorul 2

Alegem martorul 3

$3^{111} = 3\cdot 9^{55} = 27\cdot 81^{27} \equiv (-43)\cdot 94^{13} \equiv (-28)\cdot 139^{6} \equiv (-28)\cdot(-80)^{3} \equiv 10\cdot 156 = 1560 \equiv -1 \pmod{223}$

$\left(\frac{3}{223}\right) = -\left(\frac{223}{3}\right) = -\left(\frac{1}{3}\right) = -1 \equiv 3^{\frac{223-1}{2}} \pmod{223} \Rightarrow$ 223 trece testul pt. martorul 3

Alegem martorul 5

$5^{111} = 5\cdot 25^{55} \equiv 125\cdot(-44)^{27} \equiv 75\cdot(-71)^{13} \equiv 27\cdot(-88)^{6} \equiv 27\cdot(-61)^{3} \equiv (-86)\cdot(-70) \equiv -1 \pmod{223}$

$\left(\frac{5}{223}\right) = \left(\frac{223}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{8}{8}} = -1 \equiv 5^{\frac{223-1}{2}} \pmod{223} \Rightarrow$ 223 trece testul pt. martorul 5

În concluzie, nr. 223 este prim cu o probabilitate de cel puțin 87,5%.

10.39) factorizare $n = 14039$. Folosim metoda Fermat.

$\sqrt{1.40.39} \mid 118$

$1 \qquad 21\cdot 1 = 21$

$=40 \qquad 228\cdot 8 = 1824$

21

1939

1824

$=115$

$t = [\sqrt{14039}] + 1 = 119$. $t^2 - n = 14161 - 14039 = 122 \neq s^2$

$t = 120$. $t^2 - n = 14400 - 14039 = 361 = 19^2$

$n = 120^2 - 19^2 = (120+19)(120-19) = 139\cdot 101$