Cuprins

Introducere

BIECTELE CELE MAI SIMPLE studiate în matematică sunt numerele naturale. Ce poate fi mai simplu decât un număr întreg? La o vârstă fragedă ne familiarizăm cu numerele întregi, aranjate frumos în sir crescător, $1, 2, 3, 4 \ldots, 1000$, etc. Apoi ne obişnuim cu operaţia de adunare, scădere, înmulţire şi împărţire. Împărţirea de obicei are şi rest, dar dacă numărul pe care-l împărţim a fost confecţionat în prealabil din două numere înmulţite între ele, atunci acesta poate fi împărţit şi fără rest la măcar câteva numere.

Şi uite aşa apar şi primele dificultăţi: cum recunoaştem dacă un număr nu are nici un divizor (în afară de 1, şi de el însuşi bineînţeles)? Dacă numărul este mic, să zicem 23, testăm împărţirile cu numerele mai mici decât el. Dar dacă numărul este:

10000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000453.

Poate părea surprinzător dar există metode, algoritmi suficient de performanţi care pot decide şi despre acest număr. El nu are nici un divizor, este

cel mai mic număr prim cu 1000 de cifre.

Dacă descoperim însă că un număr nu este prim, – există metode care certifică acest fapt, fără a arăta concret un factor al numărului – atunci poate urma problema mai grea: cum arată descompunerea numărului respectiv în factori?

Poate părea din nou paradoxal, dar această problemă este mult mai grea. Iată aici spre exemplu un număr cu "doar" 92 de cifre:

434555890242442375857079054940698830239876361490212761073788360773718748753907205467167553 09

Ei bine, ştim precis că acest număr este compus, are divizori proprii, dar nu suntem în stare să-i aflăm pe aceştia. Problema descompunerii în factori este mult mai grea. Atât de grea încât o putem folosi – paradoxal, cum şi neştiinţa poate fi utilă uneori – în construirea unor "lacăte" care ascund bine informaţia pe care dorim să o protejăm, pentru a fi inteligibilă doar celui căruia i se adresează...

Considerăm, că aceste puţine exemple sunt suficiente pentru a motiva continuarea studiului paginilor ce urmează.