Identificarea numerelor prime

Subțirică Florin-Ioan, 322CD

Facultatea de Automatică și Calculatoare
Universitatea Politehnică din București

Abstract. Scopul acestei lucrări este o comparație între doi algoritmi populari de identificare a numerelor prime - Fermat, respectiv Miller-Rabin - care reprezintă de fapt un test probabilistic pentru a determina dacă un număr este compus sau probabil prim.

Keywords: Fermat · Miller-Rabin · numere prime · numere compuse · numere întregi

1 Introducere

1.1 Descrierea problemei rezolvate

Un **număr natural** p > 1 se numește prim dacă : p | ab atunci p | a sau p | b, unde a, b sunt numere naturale. Aceasta este o proprietate esențială a numerelor prime, iar cele două definiții sunt echivalente pentru inelul ($\mathbb{Z}$, +, ·). Un număr prim are exact doi divizori pozitivi: numărul 1 și numărul în sine. Acești divizori sunt improprii. Un număr prim este deci nefactorizabil. Cel mai mic număr prim este 2; în afară de 2 toate numerele prime sunt numere impare. Există o infinitate de numere prime, fapt demonstrat de Euclid în Antichitate.

Opusul noțiunii de număr prim este cel de număr compus. Un număr compus este un număr întreg pozitiv care are cel puțin un divizor pozitiv în afară de 1 și el însuși. Prin definiție, orice număr întreg mai mare de 1 este fie număr prim, fie număr compus. Se poate scrie ca produs de numere prime mai mici ca el, fiind deci factorizabil. Este astfel un multiplu al altor numere de modul mai mic ca el, acestea putând fi chiar prime.

1.2 Specificarea soluțiilor alese

Pentru a rezolva problema dată, am ales următorii algoritmi:

1. Metoda Fermat : Dacă un anumit număr este prim, atunci această metodă returnează întotdeauna 'true'. Dacă numărul dat este compus (sau non-prim), atunci poate returna 'true' sau 'false', dar probabilitatea de a produce rezultate incorecte pentru compus este scăzută și poate fi redusă făcând mai multe iterații.

Time complexity: O(k Log n) : De reținut că funcția putere durează O(Log n).
Auxiliary Space: O(1) : Această metoda poate eșua chiar dacă creștem numărul de iterații (k mai mare). Există câteva numere compuse cu proprietatea că pentru fiecare a < n, mcd(a, n) = 1 și $a^{n-1} \equiv 1$ (mod n). Astfel de numere se numesc numere Carmichael. Testul de primalitate al lui Fermat este adesea folosit dacă este necesară o metodă rapidă pentru filtrare, de exemplu în faza de generare a cheii a algoritmului criptografic al cheii publice RSA.

2. Miller-Rabin : Această metodă este o metodă probabilistă (asemenea metodei Fermat), dar este în general preferată în detrimentul metodei lui Fermat. Testul Miller-Rabin implementează două modificări ale funcției PSEUDO-PRIME. Prima este alegerea mai multor valori selectate aleatoriu, în detrimentul folosirii unei singure baze de bază. A doua modificare constă într-o teoremă importantă a teoriei numerelor.

   Time Complexity: O(k*logn)
   Auxiliary Space: O(1)

1.3 Evaluarea soluțiilor

Metrici de performanță. Cele mai importante metrici la evaluarea performanței ale unui algoritm de identificare a numerelor prime sunt următoarele:
– timpului de căutare și memoria utilizată în timpul căutării numerelor prime;
– acuratețea programului, deoarece acești algoritmi au șanse (destul de mici) de a produce rezultate incoerente.

Testarea algoritmilor. După implementarea efectivă a algoritmilor, aceștia sunt testați pentru a rezolva eventualele erori și se calculează valorile teoretice ale complexității timpului și memoriei folosite.
Fiecare algoritm va fi testat de mai multe ori pentru fiecare set de date, pentru a măsura o performanță medie pentru fiecare categorie și o medie generală mai precisă.
Din acestea ar trebui să putem afla și acuratețea fiecărui algoritm.

Pentru a fi mai ușor de urmărit progresul algoritmilor la fiecare rulare, voi realiza tabele, care ar descrie dependența complexitate/memorie și acurateţ̦e, cât și grafice (dreptă de regresie) pentru dependențele din tabele.

References

1. https://www.geeksforgeeks.org/primality-test-set-1-introduction-and-school-method/
2. https://www.geeksforgeeks.org/primality-test-set-2-fermet-method/
3. https://www.geeksforgeeks.org/primality-test-set-3-miller-rabin/
4. https://en.wikipedia.org/wiki/Prime_number
5. https://en.wikipedia.org/wiki/Composite_number