HANDOUT

Primalidade

Durante sua vida acadêmica você provavelmente já passou pela situação de não saber se vai haver uma prova no dia seguinte. Provavelmente você recorreria ao grupo da sala em que você poderia pegar a resposta de vários alunos (sobre ter ou não ter a prova amanhã), dado que é uma prova as pessoas não se arriscam a dizer que não vai ter caso não tenham certeza que realmente a prova não está marcada para amanhã, mas por diversos motivos você acaba ganhando diversos “acho que sim”, “não me lembro, pode ter”, e só pela possibilidade de ter você decide estudar para se garantir. Para esse caso sua certeza sobre a ocorrência da prova no dia seguinte depende da quantidade de pessoas que responderam “eu acho que sim”, ou se alguém, seja lá quem for assumir o b.o e falar “não, não vai ter, essa prova vai ser tal dia”, você toma como certeza que a prova não ocorrerá amanhã.

Para a verificação de primalidade de um número, uma resposta provavelmente certa ou certamente negativa convém muito também, uma vez que certa ou não, é uma resposta rápida.

Teste de Primalidade de Miller-Rabin

Os números primos possuem alguns testes probabilísticos, sendo os mais famosos o teste de Fermat e o de Miller-Rabin.

O teste de Miller-Rabin tem os seguintes passos:

- Escolher o número ímpar que deseja checar se é primo, vamos chamar esse número de N
- Expressar N-1 como $2^s x\, d$, em que d é impar
- Escolher um número aleatório entre 2 e N, denominando-o de a.
- Calculamos $a^d (mod\, n)$. Se o resultado for 1 ou -1, o número N passa no teste e provavelmente é primo.
- Caso contrário, deve se repetir o passo anterior elevando ‘a’ de 2^1 á 2^{2-1}, d vezes. Como por exemplo:

$a^{2^1 * d} (mod\, n), a^{2^2 * d} (mod\, n), a^{2^3 * d} (mod\, n)$... Se um desses números for 1 ou -1 então N também passa no teste sendo **provavelmente** primo, se nenhum passar é **certeza** que de se trata de um número ímpar composto.

Confuso?? É.... um pouco. Vamos ao exemplo!!

- Vamos escolher o número 13, um ímpar que sabemos que é primo, vamos checar se esse teste funciona mesmo.
- Reescrevemos o número 12 (13-1), como: $2^2 x\, 3$. Ou seja, nosso s vale 2 e o d vale 3, lembrando que d deve ser sempre ímpar.
- Um número aleatório entre 2 e 13 ? Vamos pegar o 4, logo 4 é o nosso a.
- Aplicando as fórmulas do teste:
  - $4^{2^0 * 3} (mod\, 13) = 64 (mod\, 13) = 12$
  - $4^{2^1 * 3} (mod\, 13) = 4096 (mod\, 13) = 1$
- Opa... obtivemos um número 1! Logo o 13 passa no teste de e o algoritmo o considera como sendo provavelmente primo.

Esse foi um breve resumo exemplificado do teste de Miller-Rabin. Mas o que fazer para aumentar a certeza da resposta? E se um número ímpar composto passar no teste?

Veremos a seguir....

DINÂMICA

Lembra do passo em que se escolhe um número aleatório entre 2 e N (variável ‘a’) ? Utilizando o dado entregue, os valores da tabela abaixo, e o código proposto (https://repl.it/@pedrodelapena/TestePrimo) verifique pelos valores de ‘a’ da tabela abaixo, se o número 63149 é primo:

Número tirado no dado	Número para o código
1	51309
2	17346
3	31919
4	50138
5	58891
6	44693

O número é primo? Qual foi a estratégia utilizada?

Espere instruções para a próxima etapa! Favor não continuar!

Demonstração de eficiência:

A eficiência fica mais evidente para números primos grandes, sugerimos 179426341 como um número bom para teste, mas fique a vontade para checar outros também:

Link do algoritmo convencional:
https://repl.it/repls/FirebrickFrequentCompilerbug

Link do teste de Miller-Rabin:

https://repl.it/repls/LikableNearFlashmemory

Por hoje é só ^^