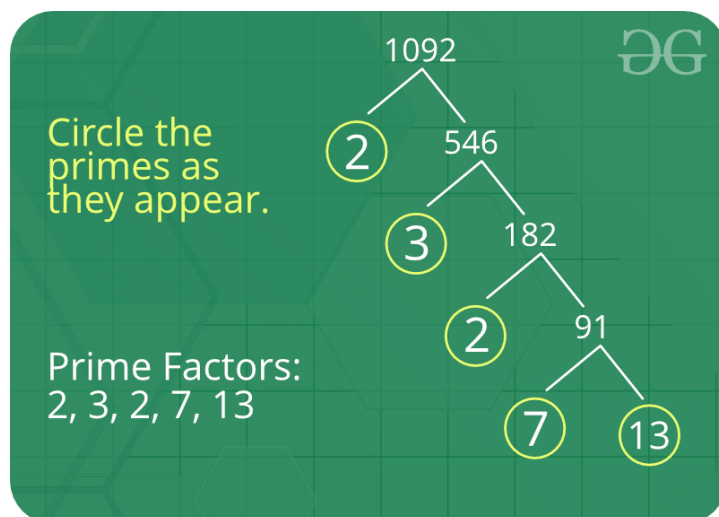




Numrat Prim

FAKTORIZIMI PRIM I NUMRAVE



Faktoret Prim te nje numri natyror

Numrat Prim

Nje numer Prim (i thjeshte) eshte numri natyror me i madh se 1, i cili plotpjestohet vetem nga numri 1 dhe vetja. Gjithe numrat e tjere quhen te perbere (composite number)

Te paret numra prim te serise jane: 2, 3, 5, 7, 11, 13, and 17 ..., Per me teper mund te shihni ne [prime number chart](#).

Numri 1 nuk konsiderohet numer prim. Ndoshta eshte e parakohshme ta themi, por numri 1 krijon nje mosperputhje me Teoremen themelore te Aritmetikës, e cila thote se:

Ekziston vetem nje set unik (bashkesi unike!) i faktoreve prim per cilindo numer.

Teoremes i jemi referuar para se te tregojme programet ne gjuhen C++.

Per me teper, ne kanal in Youtube Numberphile keni nje material interesant per kete çeshtje ne adresen:

https://www.youtube.com/watch?v=IQofiPqhJ_s&t=78s

Faktoret Prim

"**Faktoret prim**" te nje numri te perbere, jane numrat prim, te cilet te cilet shumezohen se bashku per te dhene numrin e perbere:

Faktorizimi Prim

"Faktorizimi Prim" eshte teknika algoritmike qe gjen **faktoret prim** e nje numri natyror te dhene.

Ja disa shembuj te thjeshte:

Shembull 1: Cilet jane faktoret prim te numrit 12 ?

Është më mirë të filloni të punoni nga numri më i vogël prim, i cili është 2, kështu që le të kontrollojmë:

$$12 \div 2 = 6$$

Po, është ndarë në mënyrë të barabartë me 2. Ne kemi hedhur hapin e parë!

Por 6 nuk është numër prim, prandaj duhet të shkojmë më tej. Le të provojmë përsëri 2:

$$6 \div 2 = 3$$

Po, kjo funksionoi gjithashtu. Dhe 3 është një numër prim, kështu që ne kemi përgjigjen:

$$12 = 2 \times 2 \times 3$$

Siç edhe duket, **çdo faktor** është **numër prim**, kështu që zgjidhja është e sakte.

Shenim: $12 = 2 \times 2 \times 3$ mund të shkruhet edhe me eksponent $12 = 2^2 \times 3$

Shembull 2: Cilet janë faktoret prim të numrit 147 ?

A mund ta ndajmë 147 në mënyrë të plotë me 2?

$$147 / 2 = 73\frac{1}{2}$$

Jo nuk mundet. Përgjigja duhet të jetë një numër i plotë, ndersa $73\frac{1}{2}$ nuk është. Le të provojmë numrin tjetër të thjeshtë, 3:

$$147 / 3 = 49$$

Kjo funksionoi, tani ne provojmë faktorizimin e 49, dhe zbulojmë se 7 është numri më i vogël i thjeshtë që funksionon:

$$49 \div 7 = 7$$

Dhe kjo është aq sa duhet të shkojmë, sepse të gjithë faktorët janë numra prim.

$$147 = 3 \times 7 \times 7$$

(ose $147 = 3 \times 7^2$ me eksponent)

Shembull 3: Cilet janë faktoret prim të numrit 17 ?

Pa dale pak ... **17 është numer prim.**

Keshtu faktoret prim te nje numri prim eshte vetja e tij.

$$17 = 17$$

Nje metode tjeter

Më sipër ju treguam se si të bëni faktorizimin duke filluar me faktorin prim më të vogël dhe duke vazhduar lart.

Por nganjëherë është më e lehtë të ndash një numër në faktorë (prim dhe jo prim) kurse me pas duhet të gjeni mes faktoreve te numrit vetem ata që janë prim.

Shembull: Cilet jane faktoret prim te numrit 90 ?

Zberthejme 90 ne 9×10

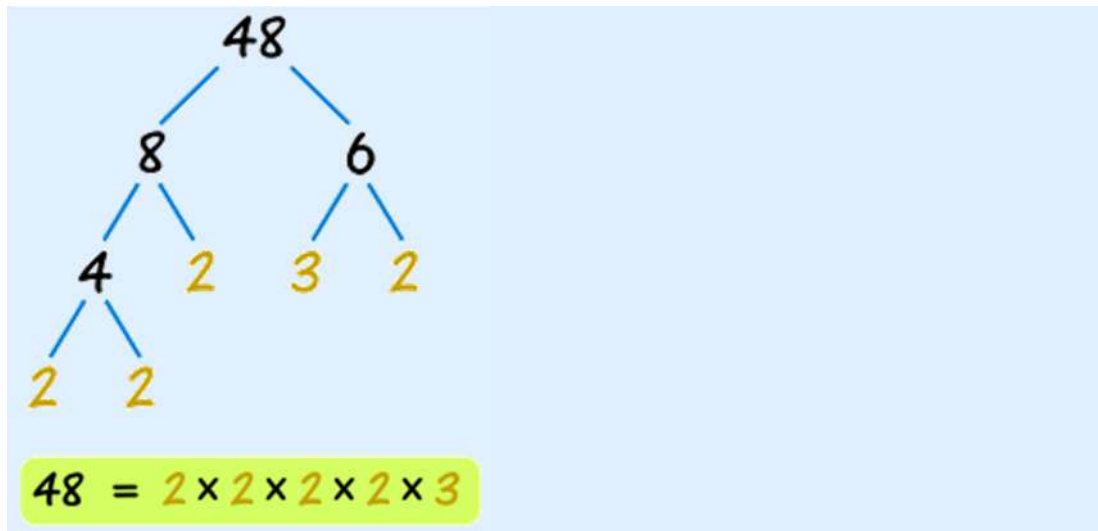
- Faktoret prim te numrit 9 jane **3 dhe 3**
- Faktoret prim te numrit 10 jane **2 dhe 5**

Keshtu qe faktoret prim te numrit 90 jane **3, 3, 2 dhe 5**

Pema e faktoreve

Nje menyre e thjeshte e faktorizimit prim eshte perdorimi i "Pemes se Faktoreve" me ane te se ciles gjendet faktoret e nje numri. Kur themi faktoret e nje numri nenkuptojme ata numra qe plotpjesetojne numrin tone. Por kujdes, jo te gjitha faktoret e nje numri, jane faktoret prim te tij. Pasi kemi gjetur te gjitha faktoret, duhet te eliminojme faktoret jo prim dhe te mbajme vetem faktoret prim te atij numri.

Shembull: Numri 48



48 = 8 × 6, keshtu qe i shkruajme faktoret "8" dhe "6" poshte 48

Tani vazhdojme me faktoret e 8 qe jane **4 × 2**

Pastaj 4 ka si faktore **2 × 2**

Se fundmi faktori 6 ka **3 × 2**

Me tej nuk mund te faktorizojme pasi te gjitha faktoret fundore jane prim.

Ne fund themi qe faktoret prim te numrit jane **48 = 2 × 2 × 2 × 2 × 3**

(ose **48 = 2⁴ × 3** duke perdorur eksponentet)

Perse na duhen Faktoret Prim?

Perderisa nje numer prim plotpjestohet nga numri 1 dhe nga vetja, themi se keta numra nuk mund te faktorizohen me tej!

Ndryshe ndodh per numrat e perbere (composite numbers), ata mund te zberthehen ne faktore prim.

Duket qarte qe numrat Prim konsiderohen **blloqet bazike te ndertimit** te te gjitha numrave te tjere (ngjashem si atomet ne kimi).

Kjo ide mund te jete shume me vlere kur punohet me numrat e medhenj, sig eshte rasti i deges se Kriptografise.

Cryptography (Fshehje/Kodim informacioni)

Kriptografia eshte dega qe merret me kodet sekrete te sigurise. Faktorizimi Prim, eshte shume i rendesishem per specialistet qe merren me gjenerimin (ose zberthimin) e kodeve sekrete bazuar tek numrat.

E gjitha kjo qe po themi ka lidhje edhe me faktin qe faktorizimi i numrave shume te medhenj, kerkon shume kohe ekzekutimi ne kompjuter.

Nese doni te dini me shume kerkoni me argumentet "encryption" ose "cryptography".

Faktoret prim te nje numri jane unik

Ne fund edhe diçka:

Ekziston vetem nje set unik (bashkesi unike!) i faktoreve prim per cilindo numer.

Shembull: Faktoret prim te numrit 330 jane 2, 3, 5 dhe 11:

$$330 = 2 \times 3 \times 5 \times 11$$

Nuk ekziton ndonje bashkesi faktoresh prim tjeter qe mund te riprodhoje numrin 330.

Kjo ide eshte kaq e rendesishme saqe u quajt **Teorema Themelore e Aritmetikes**, ose [Fundamental Theorem of Arithmetic](#).

Disa konsiderata fundore:

Kater problemet me te cmenduara te numrave te thejshte qe asnje matematikan ende nuk i ka zgjidhur.

Dega e Matematikes qe merret me numrat e thjeshte quhet Teori Numrash.

Numer i thjeshte eshte ai numer qe pjestohet vetem me veten dhe me njeshin. Numrat e thejshte jane te rendesishem sepse ata ndertojne blloqe te numrave natyror. Teorema Themelore e Teorise se Numrave thote qe cdo

4. Hipoteza e Riemann-it eshte me e famshmja dhe eshte nje problem me vleren e nje milion dollareve per ate qe e zgjidh. Kjo hipoteze eshte pergjithesim i hipotezes se numrave te thjeshte me te vegjel se nje numer i dhenei madh. Hipoteza parashton qe zerot e nje funksioni ne planin kompleks jane ne nje drejtez. Jane bere shume studime empirike (vertetime me shembuj) dhe gjithashtu eshte vertetuar per fushat e fundme, por ngelet ende e hapur per fushat e pafundme.